

1

2

3

4

5 SELECT COMMITTEE TO INVESTIGATE THE
6 JANUARY 6TH ATTACK ON THE U.S. CAPITOL,
7 U.S. HOUSE OF REPRESENTATIVES,
8 WASHINGTON, D.C.

9

10

11

12 INTERVIEW OF: CHRIS KREBS

13

14

15

16 Thursday, December 9, 2021

17

18 Washington, D.C.

19

20

21 The interview in the above matter was held in room 1540A, Longworth House
22 Office Building, commencing at 10:01 a.m.

23 Present: Representatives Lofgren and Raskin.

1

2 Appearances:

3

4

5

6 For the SELECT COMMITTEE TO INVESTIGATE

7 THE JANUARY 6TH ATTACK ON THE U.S. CAPITOL:

8

9 [REDACTED], CHIEF INVESTIGATIVE COUNSEL

10 [REDACTED], SENIOR INVESTIGATIVE COUNSEL

11 [REDACTED], SENIOR INVESTIGATIVE COUNSEL

12 [REDACTED], CHIEF CLERK

13 [REDACTED], ADMIN ASSISTANT AND SCHEDULER

14 [REDACTED], RESEARCHER

15

16 For the U.S. DEPARTMENT OF HOMELAND SECURITY:

17

18 JOHN LUCE, ATTORNEY ADVISOR, OFFICE OF GENERAL COUNSEL

19 JACKSON EATON, COUNSELOR TO THE GENERAL COUNSEL, OFFICE OF GENERAL COUNSEL

20 VICTORIA RAPPAPORT, ATTORNEY ADVISOR, OFFICE OF GENERAL COUNSEL

21 ELIZABETH O'CONNOR, ASSISTANT CHIEF COUNSEL, IMMIGRATION AND CUSTOMS

22 ENFORCEMENT, DETAILED TO OFFICE OF GENERAL COUNSEL

1

2 For CHRIS KREBS:

3

4 JIM WALDEN

1

2 [REDACTED] Good morning, Mr. Krebs. My name is [REDACTED] I'm senior
3 investigative counsel for the select committee investigating the January 6th attack on the
4 Capitol.

5 With me here -- I'll let counsel that are here introduce themselves.

6 [REDACTED] Good morning, Mr. Krebs. I'm [REDACTED]. I'm the chief
7 investigative counsel to the select committee.

8 [REDACTED] Good morning. I'm [REDACTED] I'm senior
9 investigative counsel on the committee.

10 [REDACTED] And I noticed that at least one of our members, Ms. Lofgren, is on
11 the Webex. I will attempt during the course of the day to keep my eye on that and
12 advise you and recognize the members as they come. Not necessarily as they drop off,
13 because they may be coming and going and that might be a challenge for me, but I'll do
14 my best to make sure that you're clear as to who's here from the select committee.

15 If I could ask, Jim, could you introduce yourself for the record?

16 Mr. Walden. Yes. Jim Walden. I'm Chris' counsel.

17 [REDACTED] And John?

18 Mr. Luce. John Luce with the Department of Homeland Security.

19 [REDACTED] And, John, do we have some of your colleagues on the Webex as
20 well?

21 Mr. Walden. We do. Jackson Eaton and Victoria Rappaport I see are on
22 Webex.

23 [REDACTED] So, Mr. Krebs, this is -- it's not a deposition, you're not under oath,
24 but everything that we say during this interview is being taken down by the reporter to
25 your right, and there will be a verbatim transcript created after the interview is

1 completed.

2 You'll -- we'll send a copy to Mr. Walden. He'll have a chance to go over it with
3 you and make sure that it's accurate. Just wanted you to be aware of that.

4 Mr. Krebs. Got it.

5 [REDACTED] Because we're creating a verbatim transcript, it's important that a
6 couple of ground -- we follow a few ground rules. One is that we not talk over one
7 another.

8 Mr. Krebs. Uh-huh.

9 [REDACTED] One is that we have audible responses, not uh-huhs or shakes of the
10 head, and just try and do our best to make sure that the reporter can hear us clearly and
11 create an accurate record of our interview.

12 Mr. Krebs. Understood.

13 [REDACTED] Okay. You are not -- as I said, you're not going to be placed under
14 oath today or you're not under oath today, but this is a Federal proceeding, and you're
15 required to tell the truth in a Federal proceeding. And if you were to make a knowingly
16 and willfully false statement, you could subject yourself to criminal punishment under
17 Section 10001 of Title 18. Are you aware of that?

18 Mr. Krebs. I am now, yes.

19 [REDACTED] And that is an admonition we give to all witnesses, not to you
20 specifically because of any expectation that you'll be anything other than truthful.

21 Mr. Krebs. Understood.

22 [REDACTED] We're going to -- if you need a break at any time to talk to
23 Mr. Walden or otherwise, just let me know. If a question that I ask is not clear and
24 you're not sure exactly what I'm asking, please stop me, ask me to reframe it, rephrase it,
25 and I'll do that. Sound good?

1 Mr. Krebs. Yes.

2 [REDACTED] Okay. I'm going to be taking the lead with the questioning, but over
3 the course of the interview, others may jump in with their -- [REDACTED] or [REDACTED] may jump in
4 with questions, and the members may have questions as well.

5 And from time to time -- and I note that Mr. Raskin has now joined us. I see
6 Ms. Lofgren -- oh, she's still on as well. The list is longer. I have to figure out how to
7 make sure we stay so that we can see the entire list of participants.

8 [REDACTED] The new ones pop up on the top, so we'll be okay.

9 [REDACTED] So Mr. Raskin is here. Ms. Lofgren is here. They may have
10 questions, and other members that join may have questions from time to time. And I'll
11 pause during the course of the questioning to give them an opportunity to raise any
12 questions that they have.

13 Any questions for me before we start?

14 Mr. Krebs. I don't have any at this moment.

15 [REDACTED] John, do you have something you want to put on the record before
16 we start?

17 Mr. Luce. Yes, just one brief statement. Thank you.

18 The Department has made available to the committee, consistent with requests
19 from the chairman, information and records that the Department would not publicly
20 release. This includes information and records covered under the Privacy Act,
21 personnel, and other personal privacy information, for official use only, intelligence and
22 law enforcement-sensitive records, and raw intelligence information.

23 While the Department has made this information and records available to the
24 committee, the Department asserts that such information and records provided to the
25 committee and any discussion of such information or records during the course of the

1 transcribed interview is not intended for public disclosure.

2 DHS is not waiving any protections, and for the purposes of administrative
3 efficiency and to promote constructive dialogue during the transcribed interview, is
4 making this assertion at the outset of the interview, to preserve all assertions and
5 protection from public release or disclosure over information or records used or
6 discussed during the interview.

7 The transcript and any attachments are protected from further dissemination to
8 the same extent as the documents and information they are based on. Please consult
9 with the Department prior to any public release or disclosure.

10 Thank you.

11 [REDACTED] Thank you.

12 [REDACTED] [REDACTED] sorry, one thing before you start. There's a [REDACTED] number
13 ending [REDACTED] Can you identify yourself?

14 Mr. Krebs. This is Elizabeth O'Connor. I'm a colleague of John's at the
15 Department.

16 [REDACTED] Thank you, Elizabeth.

17 EXAMINATION

18 BY [REDACTED]

19 Q Mr. Krebs, can we start with just a brief -- some brief background questions.
20 Can you describe your educational background?

21 A I went to the University of Virginia, graduated in '99, environmental sciences,
22 bachelor of arts. Moved up to D.C., went to George Mason Law School, now the
23 Antonin Scalia Law School, evening programs for 4 years, finished up there in 2007.
24 Passed the bar here in Virginia that summer, sworn in and an associate member of the
25 Virginia Bar.

1 Q And can you describe briefly your professional experience before joining the
2 Department of Homeland Security in 2017?

3 A So prior -- well, during law school, I was a contractor to the Department of
4 Homeland Security and the predecessor to CISA, the National Protection Programs
5 Directorate, I think, or it was PREP at the time, up until 2007. 2007, then I switched over
6 to Schedule C political appointment within the National Protection Programs Directorate
7 Office of Infrastructure Protection. I was senior adviser to Bob Stephan, the Assistant
8 Secretary for Infrastructure Protection. That ran until January of 2009, with a
9 switchover from the Bush to the Obama administrations.

10 At that point, I followed Bob, and we set up a consulting firm at Dutko Worldwide.
11 It was Dutko Global Risk Management. Did that for a couple years, and then went to
12 another company called Obsidian Analysis and was there. It was a consultancy risk
13 management company with both private and public sector contracts.

14 Left there in 2014, went to Microsoft, where I was a cybersecurity policy expert,
15 and stayed in that role until 2017, where I joined the Trump administration as senior
16 counselor to John Kelly, the first Secretary of Homeland Security in the Trump
17 administration. And I stayed in that role till approximately August of 2017, where I went
18 down as the -- where I was appointed by the President as the Assistant Secretary for
19 Infrastructure Protection. But given that role and the succession order of NPPD, I was
20 then a Senior Official Performing the Duties of the Under Secretary of the National
21 Protection Programs Directorate at the Department of Homeland Security. Also --

22 Q I'm sorry. Did you say that was a Presidential appointment?

23 A Yes, that was a PA.

24 Q Appointed by President Trump?

25 A Yes, that's correct. Yes.

1 Q Sorry to interrupt.

2 A It was -- within NPPD at the time, there was a PAS, and so the Under
3 Secretary was a Senate-confirmed PAS. The Assistant Secretary was a PA, so
4 Presidentially appointed with a commission and all that. And the other Assistant
5 Secretary for Cybersecurity and Communications, who's Jeanette Manfra at the time.
6 That was simply a Schedule C. That has since changed due to the Cybersecurity and
7 Infrastructure Security Agency Authorization Act.

8 So that was 2017. I was then nominated in February of 2018 to be the Under
9 Secretary of NPPD. I was confirmed June 23rd, I believe, of 2018, as the Under
10 Secretary. That job then changed November 16th of 2018, when President Trump
11 signed the CISA Act into -- into law. And then 2 years and 1 day later, November 17th,
12 7:05 p.m., fired by a tweet.

13 Q Thank you for that concise and thorough recitation of your background.
14 It's very helpful.

15 When did you start -- I take it that your work at NPPD included things other than
16 election security.

17 A That is correct. In fact, when I came in to the Department in 2017, I was
18 really, I don't think, fully appreciative of the amount of work on the election security side
19 that I would be doing. I was thinking more broadly just general cybersecurity, whether
20 it's Federal cybersecurity work, critical infrastructure.

21 But the mission of NPPD is broader than purely cybersecurity. It's actually risk
22 management for critical infrastructure in general. So that includes physical security,
23 cybersecurity, and emergency communications.

24 And the threat model that we contend with or they contend with at CISA is all
25 hazards. So it's technology risk, it's man-made risk, and it's natural disasters. In fact, in

1 2017, as the acting -- or the SOPDUS, the Senior Official Performing the Duties of the
2 Under Secretary, the majority of my fall from 2000 -- I'm sorry, from August through,
3 frankly, December, was spent with hurricane response. And so that was Harvey, Irma,
4 and Maria. And --

5 Q Those were colleagues of yours? I'm kidding. I'm kidding.

6 A Hurricanes Harvey, Irma, and Maria, and spent a fair amount of time. I
7 think I actually went to Puerto Rico three or four times. In fact, I was on the ground in
8 Puerto Rico the Monday after landfall, where the majority of the power was still out
9 across the island and which continued for some time, and then also led a congressional
10 delegation down. And, in fact, on that congressional delegation was the now Vice
11 President.

12 So it was at that point at the kind of conclusion of hurricane season where I had a
13 chance to reassess where we were as a component, as an agency. And at the time,
14 there had been a number of election security-related activities.

15 In fact, September 21st, I believe it was, 2017, is when I think the -- I'm trying to
16 get the right adjectives here. It's when the Department sent out a series of notifications
17 to State officials about what was then known as the 21 States which were targeted by the
18 Russians in the 2016 election.

19 And so through the course of the remainder of 2017 and then into 2018, January
20 or so, February really is when I think we really ramped up our election security work with
21 a dedicated task force, dedicated ISAC. Working with a multi-State ISAC in upstate New
22 York, we hosted a top secret classified briefing with election officials. It was actually the
23 same day the Department of Justice indicted a series of Russian actors for -- well, it was
24 indicted or sanctions. Anyway, it was literally, we were sitting outside the intelligence
25 community campus about to go into a meeting when the Attorney General and the FBI

1 Director made the announcement. So that was February of 2018.

2 Q So is it correct to say that prior to late 2017, election security hadn't been a
3 professional focus of yours, or am I overstating that?

4 A I think that's accurate. I think in my time at Microsoft, I was tangentially
5 associated with some election security work, because a lot of the activity that was -- some
6 of -- rather, some of the activity associated with the 2016 election interference, targeting
7 the DNC and other things, Microsoft saw some of that through their own visibility and
8 telemetry and research.

9 So -- but it is, I think, accurate to say that it was not a professional focus.

10 Q And NPPD was not -- that was an area -- that was not an area of focus for
11 you at NPPD prior to late 2017?

12 A It was -- it was as -- it was an area of focus for NPPD. There in 2016, I
13 believe -- this was, of course, before my time there. But in 2016, the summer of 2016, I
14 think that's when the prior administration and the leadership under Jeh Johnson and
15 Suzanne Spaulding and others, you know, under -- you know, came to appreciate what
16 was happening. And they started to try to figure out how to work with State and local
17 officials, and then we kind of picked up that mantle. But, again, it was not a -- of the
18 broad set of issues I had to consider coming into that role in August of 2017, it was -- it
19 was one of many, but it did become a significant focus.

20 Q And starting from the time that you mentioned in late 2017 into early 2018,
21 from that time forward to the time you left the Agency, would you say it was your
22 primary focus?

23 A It became the primary focus over time, particularly as we got closer to 2020.
24 In the -- in late January-early February of 2019, after the 35-day government shutdown, I
25 issued a set of Agency priorities. And there were five of them: Federal networks,

1 election security, physical security, control sys -- yeah, control system security and supply
2 chain security. Those were the five areas of focus, and election security was at
3 the -- typically, I would mention that second to emphasize the importance of the issue.

4 Q And is it possible for you to estimate in that sort of -- after the government
5 shutdown, after you had sort of listed those priorities till the time you left CISA, roughly
6 how many employees within CISA were focused on election security as a primary
7 responsibility?

8 A So there was the 2018, the midterm election, where we had an election
9 initiative. We had a task force that was focused on those issues. So it was -- it wasn't
10 just 2019 where all of a sudden it became a priority. It was, in fact -- it was in 2018
11 going forward to the election. And, in fact, Kirstjen Nielsen was a big part of helping
12 build that focus up within the Agency.

13 I'd say at the time the number of people -- so 2018, we actually ran some numbers
14 around this. I don't have the -- I don't recall the specifics, but it was somewhere on the
15 order of October 2018 in the run-up to the election, over the course of that month
16 anywhere, you know, around about 700 employees within CISA had done some sort of
17 election security work. And that includes field personnel, so the Protective Security
18 Advisors that are distributed across the country, the cybersecurity advisers, the other
19 staff that are out there.

20 We had elect -- we had exercise personnel that were running a series of tabletop
21 exercises. We had folks in the threat hunting team. So there was a significant amount
22 of people. And so 700 actually probably is about a third. I'd have to go back and
23 double-check those numbers. It was in the multiple hundreds. It was anywhere from
24 400 to 700, somewhere in that range.

25 Q And those, you're not counting State and local election officials?

1 A No, no, no. That's CISA Federal employees.

2 Q Okay. And did that number -- and, again, I'm not holding you to an exact
3 number, but did that sort of order of magnitude number persist through the 2020
4 election?

5 A Well, we did after 2018. So at the tail end of 2018 election, the midterms,
6 there was an Executive Order 13848 signed in by the President that directed the Director
7 of National Intelligence -- and this is important for two reasons.

8 The President directed the DNI to conduct a threat assessment of foreign
9 interference, and then the second piece of that is the 2A and 2B report. So that
10 executive order directed the Attorney General and the Secretary of Homeland Security to
11 conduct a materiality assessment, based on that threat assessment and the activities,
12 what was the material impact upon the election.

13 So we issued that report in December and January of 2018, in the midst of the
14 shutdown. Actually, I had to bring people in off furlough or whatever we were calling it
15 to conduct that. Geoff Hale and -- I'm sorry. I'm thinking back to the letter.

16 Q That's okay.

17 Mr. Luce. That's okay.

18 Mr. Krebs. So it's just 14, don't --

19 Mr. Luce. Oh, yeah.

20 Mr. Krebs. Names.

21 Mr. Luce. Oh, yeah. For names, yes.

22 Mr. Krebs. Okay. I think he's a -- okay. So there were personnel. Matt
23 Masterson who was an SES, he actually led that, led that work.

24 So we issued that assessment. And then at that time, because of the -- because
25 of the government shutdown, it was a natural kind of break point to reassess where we

1 were. And a lot of those detail -- a lot of the people that were doing the election work
2 in 2018 were detailees from other parts of, whether the Agency or NPPD at the time or
3 the Department, including the Intelligence and Analysis.

4 And so as we got through '18 and we did our own kind of internal hotwash and
5 after action review, and we restructured from the Elections Task Force to the Election
6 Security Initiative. And that launched in '19, much more focused. It resided within the
7 National Risk Management Center.

8 And some of the -- some of the people were the same, but then we swapped in
9 new -- new personnel, and we had -- again, you know, there were still some I&A folks
10 there as well.

11

BY [REDACTED]

12 Q But the several hundred -- you estimated 700, but multiple hundreds of folks
13 continued to do election security work through '19, 2019 and 2020?

14 A So the key here is that, through the course of a workweek, a Protective
15 Security Advisor or a cybersecurity adviser could go do a physical assessment of a dam
16 and the then the next day could go meet with an election official to talk about --

17 Q Sure.

18 A So I wouldn't say that 100 percent FTE on those issues. Now, I think it's
19 also -- you know, as 2019 ramped up, we were also on the heels of new secretaries of
20 state, new governors coming in, because of their own elections. And so it would have
21 been kind of a sine wave of activity.

22 But was it at the same pace of 2018? No. It was -- it -- you know, in '19 we kind
23 of, again, reassessed what -- because we had scarce resources, so we had to kind of figure
24 out, all right, what do we need to refocus on? Election security remains a priority. We
25 got additional funding in. We were able to stand up a variety of -- go ahead, sorry.

1 Q So I just want to get a sense of whether, in terms of personnel -- and I don't
2 mean down to the FTE sort of numbers, but whether the scope of the effort
3 maintained -- you said the pace slowed down a little bit, but are we dropping down to 50
4 people or 100 people, or are we still in the several hundred people who are focusing their
5 work on election security, whether as an FTE or not?

6 A So let's back off the focusing the work, right?

7 Q Okay.

8 A Was it a part of a job description among other duties for several hundred?
9 Yes. You know, was it a full-time job? I would say -- again, I'd have to go back and
10 check some of those numbers, but it could be anywhere from, you know, full time,
11 30-plus people. So it was a step back, reassess where we are, refocus our efforts and
12 restructure our efforts, and then get ready for the push into 2020.

13 Q Okay. And did things ramp up towards 2020 or --

14 A Absolutely, yes.

15 Q In terms of personnel?

16 A Yes. Yep. So we would -- so the way it worked is -- and it's not in the
17 materials, but I have a copy of it. I was just flipping through some stuff the other day.
18 We released a strategic plan for Protect2020 in I think it was January 2020.

19 The way it worked is we actually had an escalation ladder as we got closer to the
20 election. So there was the core team. They would be doing the content development,
21 the regular engagement with NASED, which is National Association of Secretaries of -- or
22 State Election Directors, and the National Association of Secretaries of State. We would
23 have exercise people.

24 As we got closer to 2020, we started ramping up. So this team would come in
25 and help support a specific effort. But as we got into, for instance, the primaries, we

1 went to a different posture where there were personnel in the -- what's now the CISA
2 Central and the Integrated Operations Division that were focusing more frequently on
3 election activity. As we backed off of primary season, then they would kind of return to
4 their regular duties. And so it's similar to kind of a military construct where as activities
5 ramp up, we bring more people in. As they ramp back down, we deescalate and they
6 return.

7 And over the course of the summer, I think we -- again, I'd have to go back and
8 look at the ops plan, but I believe we started going to that more active posture in
9 September of 2020, where we had significant additional support, from a monitoring
10 perspective and a coordination perspective.

11 Q Got it. Okay. Let me back up a little bit in terms of the -- you talked a
12 little bit about the predecessor agency and then the creation of CISA. Can you just talk a
13 little bit about your understanding of the impetus for creating CISA as a freestanding
14 agency -- not freestanding, but creating CISA?

15 A Operational agency within DHS.

16 Q Yes.

17 A So it had been, as I understand it, at least an effort that had been underway
18 since probably 2010. Rand Beers, who was the Under Secretary then, you know, that
19 was one of his key recommendations. So they pushed for it.

20 Suzanne Spalding, my immediate predecessor, came in and she made a big push
21 for it in the 2015 -- '14, '15, '16 time. Couldn't get across the finish line.

22 For me, it was my top priority coming into the administration, at least into DHS.
23 Worked with the leadership, whether it was Secretary Kelly or then-Secretary Nielsen
24 afterwards, had full support from the administration.

25 My -- you know, I thought it was critically important for a couple different reasons.

1 It was recruiting. It was actual public engagement. Showing up and saying, hey, we're
2 with DHS, doesn't always work. When you go to some organizations, like schools and
3 colleges, they don't necessarily like DHS showing up. That's my opinion, by the way.

4 Others is when you try to work with a private sector partner and you say, hey, I'm
5 with the National Protection and Programs Directorate, they don't know what the hell
6 that means. And so what we really wanted was an organization that clearly and
7 concisely communicated what the mission of the Agency was, and cybersecurity right off
8 the bat.

9 So I came in --

10 Q How would you articulate the mission of the Agency when it was formed?

11 A In 2018 or --

12 Q Yes.

13 A The mission of the Agency --

14 Q Of CISA.

15 A Yeah. The mission statement, off the top of my head, I don't recall, but it's
16 effectively to help -- help critical infrastructure manage risk.

17 Q Okay.

18 A From all comers, foreign, domestic, all hazards.

19 Q Okay. And what did you understand the role of CISA to be with respect to
20 election security?

21 A So when you -- when you look at the intelligence community assessment of
22 2017, it breaks down the Russian activity in 2016 into three buckets. First is targeting of
23 election equipment; the second is targeting campaigns; and the third is just a broader
24 disinformation, you know, disinformation efforts that the Russians have been doing for a
25 century or more.

1 In terms of the bidding internal to the U.S. Government on who had lead in those
2 three areas, it was clear, you know, once Jeh Johnson, the prior Secretary in 2017,
3 January of 2017, designated election infrastructure critical infrastructure, it was, you
4 know, CISA had the lead for working with State and local election officials on protecting
5 critical infrastructure -- or election infrastructure. That's the systems. That's the
6 hardware. That's the equipment and the processes associated with conducting an
7 election.

8 Q And so can I stop you there for a second?

9 A Yes.

10 Q Is that primarily protecting against what we would think of as hacking?

11 A No, not necessarily. It's, again, critical infrastructure, we had an all-hazards
12 approach. So we worked with election officials to conduct active shooter drills and
13 assessments. We would go look at election warehouses where equipment is stored in
14 the off season, do physical risk assessments.

15 In the wake of hurricanes, we would work with election officials. In fact, Kyle
16 Ardoin, who's the Secretary of State in Louisiana, in 2000 -- the summer of 2020, I guess,
17 where they got hit pretty hard by an election, we helped him work with FEMA and some
18 of the response efforts there to get resources he needed to be able to conduct the
19 election in 2020.

20 So it was not just cyber. That tended to be the public -- at least what the public
21 cared about or the media cared about, just because it's 2016, but it was -- again, it was an
22 all hazards. And we did -- I don't want to put numbers on it, because I don't recall,
23 again, off the top of my head, but a significant number of physical assessments of election
24 facilities.

25 Q Got it. Got it. And would that include things like -- and I don't know if this

1 is an EAC issue, but I've heard or read about the ballot paper and sort of the security
2 issues with respect to the type of paper that's used for ballots and things like that.
3 Would you put that in the infrastructure context or only physical machines you're talking
4 about?

5 A From the perspective of, you know, selecting paper, no, that's not a process
6 that we were involved with. If it was a -- you know, if an agency asked for advice on
7 how would we protect a logistics supply chain for paper, then we could give them some
8 advice --

9 Q Got it.

10 A -- on how to do that and how to secure the facilities, for instance, that hold
11 the ballots. But from picking paper or designing paper, things like that, that was not.
12 That was more of an administration, election administration requirement.

13 Q And picking or designing machines, any role that CISA played?

14 A So we certainly had risk management opinions about -- or perspectives,
15 rather, about the types of machines that were in use. And from a risk management and
16 resilience perspective, we strongly encouraged and, you know, even advocated to the
17 Congress on behalf of States for machines that had paper trails, so voter verifiable paper
18 audit trails.

19 If you recall, in about 2016, there was probably about little under 80 percent,
20 according to the Center for Election Innovation. The -- I think it was about just under 80
21 percent of votes cast had a paper record associated with it. There were five States at
22 the time -- Louisiana, Georgia, South Carolina, Delaware and New Jersey -- that had the
23 DREs, the direct recording equipment. So you touch the screens, it's tracked on
24 removable media.

25 Over the course of the 4 years between '16 and '20, that number -- I think the

1 number for 2020, it was around 95 percent of votes cast had a paper trail associated with
2 it. And, you know, our encouragement there was because of the auditability. And
3 auditability is resilience. And so if, you know, Georgia or something got popped, then
4 it'd be harder to -- or there were claims or actual technical interference with the DREs, it
5 would be harder to track.

6 And I think we were hugely successful in at least helping push that initiative and
7 that transformation across elections from '16 to '20. There was -- in The Washington
8 Post Cybersecurity 202 this morning, in fact, there's a -- the front matter of that piece is
9 about how Louisiana is the only State left that's statewide DREs.

10 Q That was going to be my question. Do you know in November 2020
11 which -- there may be small counties here or there, but do you know generally which
12 States had not made the transition to paper ballots?

13 A Statewide, the --

14 Q Or, no, just had jurisdictions within the State that were not -- did not have
15 paper ballots.

16 A So Georgia, South Carolina, and Delaware both made the switch over to, in
17 some cases, ballot marking devices. I know both Georgia and Pennsylvania had those.
18 So New Jersey was a State that had DREs, but due to the pandemic, they switched over to
19 absentee or mail-in balloting.

20 Louisiana -- so what remained as I understood -- understand it, rather, it was
21 Louisiana statewide, Tennessee, Indiana, Texas, and a handful of others. Now, you may
22 find DREs in a small -- in use in small amounts across the country for accessibility
23 purposes, for people that just can't use paper. But at a larger scale, it's Tennessee,
24 Indiana, Texas, and Louisiana.

25 Mr. Walden. I'm sorry. He asked you a question. I just want to make sure

1 your answer is clear. I won't do this very often, but I just want to keep track.

2 So the ones -- the only ones statewide that didn't have it was Louisiana,
3 Tennessee, Indiana, and Texas. Some locations didn't have it?

4 Mr. Krebs. Right.

5 Mr. Walden. But New Jersey, Georgia, South Carolina, and Delaware did?

6 Mr. Krebs. So in 2020, South Carolina had -- by 2020, South Carolina had
7 switched to a paper trail. Georgia had switched to a paper trail. Pennsylvania had
8 switched to a paper trail. New Jersey just chopped over to absentee. And Delaware
9 had switched as well.

10 BY [REDACTED]

11 Q Now, but -- and I understood those were switch-overs for 2020, but it's not
12 to suggest that other States throughout the country that you're not listing, those also
13 were paper. So California, Pennsylvania, Michigan --

14 A Right.

15 Q -- those were all -- those were paper as well?

16 A Yes. So, again, just to restate, for 2020, the States that had a significant or
17 substantial number of DREs, so, again, Louisiana was statewide, and then there were
18 counties or jurisdictions within Tennessee, Indiana, and Texas. Those are the ones that
19 are immediately coming to mind. And there are a handful of others, but those are
20 the -- those are the bigger vats.

21 Q Got it. So I interrupted your answer earlier to get onto the infrastructure
22 protection. You talked about sort of other -- you talked about a three-pronged --

23 A Yep.

24 Q -- concern with respect to what the Russians had done in 2016. Does that
25 sort of track to sort of the three prongs of what CISA was focused on?

1 A So on the election infrastructure, CISA had lead across the Federal
2 Government. So we would lead the engagement with State and local election officials
3 to conduct risk assessments, improve the security of their -- their systems, to conduct
4 training, coordinate, share intelligence and information. And then FBI supported us.
5 The intelligence community supported us.

6 On the second piece with campaigns, FBI generally had the lead where we would
7 support. We would provide any sort of assistance, but there was not a whole lot of
8 support requested from any of the Presidential or other Federal campaigns. They
9 were going to do their own thing and --

10 Q And when you say campaigns, what are you referring to there? I mean,
11 what's the threat or what's the issue? Infrastructure I think you've explained well, sort
12 of the risks --

13 A Right.

14 Q -- and the threats. When you say campaigns, what are you referring to?

15 A So the DNC, the RNC, the actual -- you know, the Biden campaign, the Trump
16 campaign.

17 Q But efforts by some mal actor to steal material?

18 A Correct. So in 2016, the Russians hacked into the DNC and exfiltrated email
19 and released those emails through various means. And so our -- you know, the concept
20 there was, okay, it happened before. This is part of the playbook, so we should offer to
21 those campaigns support if they need it.

22 So what we would generally do in a one-for-one bipartisan manner -- so if we
23 briefed the RNC, we briefed the DNC. If we briefed the Trump campaign, we briefed the
24 Biden campaign, or we'd at least offer it, and offer them an assessment of what we saw
25 was happening in the world.

1 Some of those briefings were classified. I never participated in any of the
2 briefings to -- so I'll say that, as far as I can remember, I think I was in one meeting at the
3 RNC with Ronna McDaniel, where we kind of just talked about elections. But, generally,
4 in -- that was the 2018 timeframe.

5 For 2020, as we ran up, it was typically -- those briefings were typically led by a
6 career official, for purposes of remaining nonpolitical.

7 Q With the goal being how to help the campaigns or the party committees
8 protect their information from --

9 A Yes.

10 Q -- intrusion?

11 A Yes.

12 Q Foreign or domestic? Did you have a -- was there --

13 A I mean, we would generally brief them because of the intelligence
14 community's, you know, purview, on foreign threats. So if we saw something coming
15 from Russia, Iran, you know, China, whatever, it would be -- you know, we would be able
16 to provide that to them to help them understand the risk landscape. But, again, that's
17 because of the information we had available. I don't think there was any domestic
18 technical information that would have -- would have come up.

19 Q But did you feel that there was some lane of authority there that you had to
20 observe in terms of where that -- the threat of intrusion might come from? So, in other
21 words, if it was a -- if it was a hacker in his parents' basement in New Jersey, is that a
22 threat that you considered part of your mandate to address and brief the campaigns on?

23 A So break things apart here. So from a threat modeling perspective, you
24 know, based on the available intelligence, those concepts would be primarily driven by
25 foreign actors. It would be, hey, here's what the Russians are doing. And a lot of that

1 was informed by things that Cyber Command was doing.

2 So Cyber Command was doing some foreign operations -- this is
3 unclassified -- foreign operations in Ukraine and other Eastern European countries where
4 they could actually observe in those networks. They'd partner with their own country.
5 They'd partner with those countries, and they'd be able to see Russian GRU activity.

6 And what we'd be able to do is we'd be able to take the techniques that they were
7 using. We'd be able to take the malware that we found or that the -- and then as well as
8 the targeting sets. And whether it was election night reporting or voter registration,
9 package that up and then turn around and share that with -- with our State
10 election -- State and local election officials.

11 We also partnered with FireEye and other cyber threat intelligence companies to
12 do the same thing. It was like, hey, this is the activity we're seeing. And because
13 they're a private sector organization, there is no domestic Fourth Amendment issues.
14 And so they were able to pull together any sort of information they saw from threat
15 actors, but they don't get too deep into the attribution game. And we'd share that.

16 So that's from a threat modeling perspective. But from a defensive posture
17 perspective --

18 Q Yes.

19 A -- it doesn't matter. Because, frankly, when you see the activity, you don't
20 know. It takes quite some time to figure out who the bad guy is most of the time. And
21 so it wouldn't have mattered for us if it was a domestic or a foreign actor. We provided
22 security advice from all comers to help them defend from any bad actor.

23 Q So, from your perspective, there was no bright line that you needed to
24 observe, in terms of advising the stakeholders, whether it's local -- State and local
25 officials, campaigns is what we're talking about now, you didn't feel that you needed to

1 back off if the perceived threat included domestic actors?

2 A From a cyber perspective, absolutely not. I mean, look, there are criminals
3 here domestically that would try to hack in. I mean, there were some investigations
4 that, I understand it, after the 2016 election related to domestic cybercriminals that were
5 trying to hack into databases and things like that.

6 So for us it was -- because the techniques aren't going to change all that much.
7 They use the same tools. And that's -- so it doesn't matter, right?

8 Q Okay. Let's -- sorry.

9 A Sorry. And there's a second piece here is that some of the techniques that
10 were used in 2016 by the Russians, it continues to today for both Russia and China. But
11 what they do, it's not like they try to come at you from a Russian IP address.

12 So you can't just say, oh, block all Russian IP space from connecting to your
13 network, because what they're doing is they're jumping around the global internet, and
14 they will pop up in domestic hosting providers. And so they'll use virtual private servers
15 that are domestic based.

16 Microsoft just did a blog on this, or FireEye -- or Mandiant and Microsoft, where
17 they would come into an area -- so let's just use -- I'll just randomly pick, say, Georgia,
18 because that's where I'm from. If they were trying -- if a bad guy is trying to go after a
19 target, so if a Russian is trying to go after a target in Georgia, what they will do is they'll
20 come in and they'll compromise hosting infrastructure in Georgia. So when you see the
21 traffic, it would look like someone that's a customer in the same city or the same town or
22 whatever. So that's just one of the techniques.

23 So you can't tell that it's Russia coming in. So, again, our advice was almost
24 agnostic to the specific actor and, instead, a defend against all threats.

25 Q Okay. But not just -- and I think I'm just restating what you said earlier.

1 But you were agnostic not just because the Russians might be posing as a Georgian in the
2 State of Georgia, but because there might be someone who actually is an American
3 citizen within the State of Georgia could be doing the same sorts of things that you're
4 worried about?

5 A So yes. And this is not specific to election infrastructure. This is all critical
6 infrastructure, right? So when we work with chemical facilities -- and there's a
7 significant chemical security effort at CISA -- we would not just be worried about al-Qaida;
8 we would be worried about a domestic actor coming in and stealing chemicals that could
9 be used for nefarious purposes. So, again, the month -- or the threat actor focus of CISA
10 is all hazards.

11 Q Got it.

12 A It is man-made, foreign, and domestic. It is natural disaster. It is
13 technology-driven.

14 Q Okay. Let me get to the third prong of the -- what I think you were
15 describing as the Russian campaign in 2016. And I think -- does it also track sort of the
16 third prong of what you were focused on --

17 A Yes.

18 Q -- from an election security standpoint?

19 A Yes.

20 Q And what's that?

21 A So the third prong is just this broader disinformation campaign that in 2016
22 had -- there was an election-related disinfo piece, but there was also a much
23 broader -- there continues to be a much broader effort by Russian influence actors to
24 destabilize the U.S., to undermine confidence in the American people in their leadership.

25 And so, you know, one of those kind of not related to election issues would be,

1 you know, they were involved in promoting both Black Lives Matter -- Black Lives Matter
2 and anti-Black Lives Matter protests and counterprotests. They boosted some of the
3 Kaepernick Nike take a knee sort of stuff.

4 But specific to elections, there was also the -- there was also the disinformation
5 related to, you know, things that were going on. So Tennessee GOP was a Twitter
6 handle, the Ten_GOP was a Twitter handle that the Internet Research Agency based out
7 of St. Petersburg used to promote election disinformation in '16.

8 So, to step back, we assess that, based on '16, they would continue to use these
9 techniques, and they did. And so as a Federal Government, this is where things are a
10 little bit looser, because disinformation is, I think, generally a more nascent national
11 security risk, that there is not a, for instance, a national security strategy for countering
12 disinformation.

13 In fact, this is a recommendation that I championed in the Aspen Commission on
14 Information Disorder, that the Federal Government needs a whole-of-government
15 strategy to understand the threat of disinformation, misinformation, and malinformation
16 to the United States.

17 And so there is no broad countering disinformation strategy. Instead, the way
18 we looked at it -- and this was coordinated through the National Security Council. But
19 the way we looked at it was to break up disinformation threats into a supply and demand
20 sort of approach.

21 And so on the supply side, again, from an unclassified perspective, you would have
22 the intelligence community, the FBI, that would be looking to understand who the threat
23 actors were. So if it's the Internet Research Agency coming out of St. Petersburg, they
24 would be able to then identify the accounts, not the content. It's all content neutral.
25 They'd be able to identify the accounts and then say, hey, we can tie this back to a

1 disinformation operator that works for the IRA. Hey, Facebook, Twitter, whomever, you
2 guys -- you ought to go check this out and investigate it.

3 And so that would then lead to an internal Facebook investigation and that they
4 could, you know, expose a coordinated unauthentic behavior campaign. So that's
5 disrupting the supply side.

6 On the demand side, where CISA sat -- and this is, in part, based on a broader set
7 of authorities related to the Department of Homeland Security, as I understood them and
8 as I was counseled consistently and constantly throughout the process, but we had an
9 awareness and education mission. And so that's the demand side. So, you know,
10 seeking to help kind of stabilize or diminish demand for disinformation.

11 So that's what led to, in 2019, the release of the -- the War on Pineapple
12 campaign, which was -- it was about July, I think, of 2019, where the idea here was we
13 would educate, based on our understanding of how foreign influence actors worked.
14 We would help educate the American people in a kind of a noncontroversial way.

15 So we broke the foreign influence operators' techniques into five steps. First is
16 identify the issue. And I can send you the graphics, the infographics. First is identify
17 the issue.

18 Second is get your accounts into place. So whether it's Twitter or Facebook.
19 Sometimes the seasoning of those accounts can take a few months or even a couple
20 years. You saw in '16 that they had had some Twitter accounts they had been using or
21 had ready to go for like 5 or 6 years. So, again, the second is you get your accounts into
22 place.

23 Third is you start boosting the issue that you want to push. Typically, that
24 happens on social media platforms and Facebook groups and things like that.

25 Fourth is you take it mainstream. That's where you want to take it out of the

1 social media platform into mainstream news and getting it to land on FOX News or
2 MSNBC or whatever your target audience is.

3 And then fifth is you actually take it to the real world.

4 And in '16, we saw them jump from Facebook groups into FOX and others. And
5 then you actually had real life protests and counterprotests and trying to get the conflict.
6 And, in part, that's what happened with January 6th, right?

7 Q Well, we're going to get there for sure.

8 A Yeah.

9 Q You called it the War on Pineapple campaign. Where does that title come
10 from?

11 A So, again, the concept here was that we wanted to have an issue that was
12 noncontroversial and understanding that there was a lot of national -- you know, anything
13 Russia could immediately set off potentially half your audience. So we tried to pick
14 something that didn't have any political connotations.

15 And so the Election Security Initiative team, again, Matt Masterson and a few
16 others, were -- you know, they got everything scoped out and they just had to figure out
17 what the issue was to -- that we would mock up. They went to lunch, had -- they were
18 trying to figure out what's a binary issue. It's like, you know, do you like salt and vinegar
19 chips or something like that. What they actually came down to is whether you like
20 Hawaiian pizza or not, and like it's a very clear-cut --

21 Q Yes.

22 A It's like you either love it or you hate it. And he is from New York, so he
23 probably hates it. Yeah.

24 So what we did was that was kind of the -- you know, it's light, it's fun, it's
25 engaging. And so that was the point of the public awareness campaign. We released

1 that in, like I said, June or July or so of '19. And then we actually pushed a Twitter -- fake
2 Twitter war. And we got National Association of Secretaries of State and the National
3 Association of State Election Directors to take opposite sides. One side liked it, the
4 other side didn't. So we pushed it. It caught on.

5 And so to the point now where any time anything happens on Twitter where
6 pineapple, you know, Hawaiian pizza, pineapple and pizza is an issue, I get tagged. And
7 so, you know, it happens at least once or twice a week. So it worked, right? We raised
8 awareness at least that pineapple on pizza is gross.

9 But to get back to the broader point here, our mission here in the disinformation
10 space was to provide information on how disinformation operations work, but also as
11 certain themes would emerge related to election disinformation, we would work with a
12 range of partners, whether it's at the State level, the Federal level, with the EAC, with the
13 Postal Service, with DOD, to provide authoritative information on what happened.

14 So I'll give you an example. 2020, October 22nd and 23rd, a series of emails start
15 popping up in people's email in-boxes throughout Florida and elsewhere. The emails
16 claim to be from the Proud Boys, and they are saying, hey -- and they tend to be targeting
17 Democrats and -- registered Democrats at least. And so the claims say, hey, we know
18 you're a registered Democrat. You have to change your registration and vote for Trump.
19 If you don't, we're going to come after you and we'll know who you voted for.

20 And so we saw these coming in. And we -- you know, the way we would
21 address -- deal with this, with any of these themes or claims is we would just
22 systematically reverse engineer the claim.

23 So the claim here is that we will know who you voted for. So it's the law of the
24 land in all 50 States of a secret ballot. That's kind of the magic of American elections.
25 And so that was the hook for us, to say, these sorts of emails are coming out. The -- it's

1 actually untrue that anyone would ever know who you voted for unless you tell them.

2 There's a secret ballot. So disregard, this is disinfo.

3 And that was the crux of rumor control, which we launched that Monday or

4 Tuesday of the week of 21, 22, whatever it was, October.

5 Q Can I stop you there for one second?

6 A Yep.

7 Q Because I know a little bit more about where this story goes, but I want to
8 pause on this piece of it for a minute.

9 The threat is a -- it's what you would describe as an influence campaign? This
10 isn't a physical intrusion into any hardware?

11 A Yes, right.

12 Q It's an effort to influence voters for some -- someone has an objective here.
13 They want voters to think a certain thing.

14 A So influence is kind of --

15 Mr. Walden. I'm sorry, hold on. What's the question?

16

BY [REDACTED]

17 Q Is that how you would characterize this, as an influence operation?

18 A Yes. That is an influence operation. I think the -- that's more of a
19 technical term that lacks the specificity of the objective. The objective here was to
20 intimidate, intimidate voters, scare voters from voting.

21 Q Okay. And, initially, you don't know who's behind this, correct? When
22 you first learn of these emails, you don't know who's behind these emails? They're
23 ostensibly from the Proud Boys, right?

24 A They're ostensibly from the Proud Boys. We need to walk carefully here.

25 Q Okay, understood. But they're ostensibly from the Proud Boys?

1 A Yes.

2 Q And you felt that this was something that fit into your mandate, in terms of
3 educating the public and addressing potential influence operations?

4 A Not only did it fit squarely in our mandate, but it was signed off, not just by
5 DHS leadership, but also White House.

6 Q Because we've heard from former DHS leadership that there was sort of a
7 jurisdictional issue here, in that CISA or DHS was supposed to be focused on foreign
8 interference and internet issues, foreign influence or internet issues. Is that your
9 understanding?

10 A Foreign -- so explain foreign influence in this.

11 Q Well, if there were an influence operation, for example, by a foreign
12 government, the Russians, say, that would be within CISA's mandate.

13 A Okay.

14 Q But a domestic actor doing the same sort of thing, like the Proud Boys, for
15 example, would not be within CISA's jurisdiction. Do you agree with that assessment?

16 A I do not agree with that assessment.

17 Q And at the time that this Proud Boys -- these Proud Boys emails came up in
18 the fall of 2020, you said that you had sort of -- you were in alignment with DHS
19 leadership and the White House on addressing this false information that was being
20 spread in Florida or elsewhere.

21 A Absolutely. In fact, we were lauded for our rumor control work that week
22 by White House leadership, including the chief of staff and the National Security Advisor.

23 Q Now, I don't want you to get into certainly any classified information, but I
24 do think you've spoken publicly or it was disclosed that it turns out it was a foreign actor
25 involved with the Proud Boys emails.

1 A It was Iran. Yes. And we went from first discovery of that email 11 a.m.,
2 noonish maybe, when reports came out on Tuesday to standing in FBI headquarters that
3 evening, Wednesday evening about 7 p.m., attributing that attack to Iranian -- that
4 influence operation to Iranian actors. And I was there in that press briefing.

5 [REDACTED] Let me pause here. I don't see that we have any members on.

6 [REDACTED] or [REDACTED] do you have any questions?

7 [REDACTED] I don't, no.

8 [Krebs Exhibit No. 1

9 Was marked for identification.]

10 BY [REDACTED]

11 Q Let's take a look at exhibit 1 in your binder, which is -- these are prepared
12 remarks, testimony that you gave before the Homeland Security and Government Affairs
13 Committee of the U.S. Senate in December of 2020. You've obviously seen this
14 document before?

15 A I may have written it, yes.

16 Q Okay. And did you have a chance to review it again before today?

17 A Yes, I've reviewed this several times.

18 Q So I want to ask you about a couple of points that you make in here.

19 A Okay.

20 Q And the first one is on this issue of sort of the -- I'm sorry.

21 Mr. Luce. I have a copy here.

22 BY [REDACTED]

23 Q Some of the issues that are raised by these foreign influence campaigns in
24 particular. And on page 2, under "The Initial Challenge," the paragraph says "Initial
25 Challenge," you say in the second sentence referring to interference campaigns by the

1 Russian Federation, that: "Whatever their other motivations, these Russian campaigns
2 sought to create chaos and division among Americans, implant disinformation, sow the
3 seeds of distrust in democratic institutions, and, in this way, degrade America's standing
4 abroad."

5 A Uh-huh.

6 Q Can you talk a little bit about how you came to those conclusions that that's
7 what they were trying to do -- or the Russians were trying to do in 2016?

8 A That is just the broader strategic objective of the Kremlin. And
9 disinformation operation is not specific to necessarily just the 2016 election, but that's
10 just their strategic approach. And this is not my -- necessarily just my opinion. This is
11 the prevailing, I think, academic and, you know, kind of Russia head approach, and it's
12 informed by, you know, folks like Thomas Rid, who's a professor at Johns Hopkins.

13 But that is -- that is the -- kind of the asymmetric strategy that they're pursuing.
14 They have entire units of the GRU that seek to operate in their, you know, European orbit
15 to conduct assassinations and things like that, again, to just destabilize the Western-level
16 democratic order.

17 Q And specifically with respect to election issues, were you concerned and did
18 you view it as your role to try to combat those types of disinformation campaigns for the
19 reasons that you've listed here in the paragraph that we're looking at; that is, to make
20 sure that an actor was not able to create chaos and division among Americans, sow the
21 seeds of distrust in democratic institutions and so forth?

22 Do you need me to repeat that?

23 A No. So the answer is yes, that is -- that was part of the integrated
24 coordinated response to Russian efforts, where there were parts of the Federal
25 Government that would more directly take on the activities. But under the assumption

1 that we would not be able to necessarily catch everything and prevent it from happening,
2 there had to be kind of a resilience measure. And that was our role, was to help explain
3 how these things happen and prepare the American people, inoculate, so to speak, from
4 these sorts of attacks.

5 Q I'm interested in hearing your perspective on why you think that's important,
6 why the American public needs to be inoculated, and what the stakes were here with
7 respect -- if they weren't.

8 A We're in a broader -- okay, so this kind of -- let's step back here again and
9 talk about things like the Aspen Commission on Information Disorder that I co-chair.

10 The challenge is we're in the midst of an information disorder where
11 they're -- disinformation, misinformation, malinformation is flying, due to technology, the
12 prevalence of technology, social media, online, you know, enabled communications
13 techniques, unlike ever before. It's the velocity of information that's happening, and it's
14 being weaponized by all sorts of actors, you know, foreign actors, domestic actors,
15 grifters, those that continue to, you know, seek dominion over others.

16 And so the point here is that we understood that the -- that the Russians primarily
17 were -- but others were doing it too -- were seeking to destabilize the United States by
18 undercutting the public's confidence in, not just the national security apparatus and the
19 government writ large, but just destabilize or undermine whatever truth is.

20 And so part of our mission was, when we understood a national security risk that
21 was impacting the United States, it was within the authorities, as we understood it,
22 particularly when it came to critical infrastructure-related issues, like election security, we
23 had a mission and the authorities to engage and provide explanatory and authoritative
24 information to counter, to inoculate, to rebut any of these election-related disinformation
25 claims.

1

2 [11:04 a.m.]

3

BY [REDACTED]

4

Q And do you feel that that understanding or --

5

A So let me -- I want to add one more piece here, again, to explain why this is not just election security, this is also about critical infrastructure protection.

7

So, in 2020, in probably about April, FEMA actually set up a rumor control site that we contributed content to. There were critical infrastructure -- telecommunications is critical infrastructure, right? Telephones, internet service providers, anything that allows you to communicate. There were claims, disinformation claims, being associated that COVID was being spread by 5G and 5G towers.

12

It's critical infrastructure. It's disinformation. We worked with scientists and telecommunications experts to provide authoritative information to FEMA that they could then put on their rumor control site that, as far as I know, is still there today on why, scientifically and technologically, that is not possible.

16

So that is a -- again, it goes to the broader critical infrastructure mission of the Department. Election infrastructure is critical infrastructure. And, as specific election-security-related disinformation claims came up, we felt it was important to provide, again, authoritative information to rebut some of the claims.

20

Q Okay.

21

BY [REDACTED]

22

Q Can I jump in and just ask -- I appreciate, Mr. Krebs, that the Department did and does a lot to counter disinformation by calling it out, identifying it, providing a counter-narrative.

25

Are there legal authorities consistent with the First Amendment that the

1 government, DHS or otherwise, uses to shut down, stifle, prevent the dissemination of
2 misinformation? There are two ways to sort of --

3 A Right.

4 Q -- combat this. You can either counter the misinformation with more
5 speech, or you can try to shut down the misinformation. Tell me a little bit about the --

6 A I can only speak to what I was involved with at CISA --

7 Q Yeah.

8 A -- but we certainly, as far as I'm aware, took no actions as a government
9 actor to censor, to --

10 Q Yep.

11 A -- to stop any speech.

12 Q You're exactly anticipating my question. There is no authority for the
13 government to censor, to stifle, to prevent foreign or any actors from disseminating this
14 kind of blatantly incorrect misinformation.

15 A We -- again, our --

16 Mr. Walden. I'm sorry. I just want to make sure, because we have a record
17 here, your question is, does he know of any legal authority --

18 [REDACTED] Yeah,

19 Mr. Walden. -- to shut it down? Okay.

20 [REDACTED] Legal authority or action to do so.

21 Mr. Walden. Okay.

22 Mr. Krebs. I am not aware of any action CISA took to shut down speech --

23 BY [REDACTED]:

24 Q Right.

25 A -- right? -- any direct action we took.

1 There were circumstances where we connected State officials in the 2018
2 election, State of Ohio, connected State officials with social media platforms --

3 Q Uh-huh.

4 A -- so that, if the State official said, hey, there's a video about a -- there's a
5 video on whatever social media platform that seems to show a vote being flipped, we'd
6 like to talk to Facebook or Twitter, whatever -- I can't remember the platform -- about
7 that and share our perspective and our facts on what's happening in the video, we
8 connected them. We had, beyond that, no activity.

9 Q Yeah. So the purpose of a conversation like that would be so that the
10 platform could potentially flag, deplatform, or restrict the --

11 A Do whatever, right.

12 Q Do whatever --

13 A Yes.

14 Q -- its terms and conditions of --

15 A With their terms of services, right?

16 Q Exactly.

17 A Yes.

18 Q Okay.

19 A But, again, the Federal Government was not taking direct action --

20 Q Yeah, I understand.

21 A -- other than connecting parties.

22 Q I just want to sort of understand what the various levels are that we,
23 collectively, we, the U.S. Government --

24 A Yeah.

25 Q -- have to combat this.

1 A So there are other levers that other -- you know, again, I'm not speaking as a
2 source of authority here, but, based on my understanding of the research, there are other
3 agencies that may have fraud-related -- you know, FTC took action against --

4 Q Yeah.

5 A -- some of the pandemic grifters for, you know, alternative therapies early in
6 COVID. But, again, from a CISA perspective, you know, there are no affirmative
7 authorities that we have that we could proactively use.

8 Q Okay. That's it. Thank you.

9 Sorry to interrupt.

10 [REDACTED] No. No problem.

11 BY [REDACTED]

12 Q You reference in this document, exhibit 1, several times taking measures to
13 protect the public's confidence in the election system in this country. Do you
14 understand that to be or did you understand that to be one of the missions of CISA?

15 A Restate the question, please.

16 Q Did you understand one of the missions of CISA to be to promote and
17 protect the public's confidence in the elections in this country?

18 A I believe that is a byproduct of our mission, and the mission being providing
19 authoritative information on the security of elections to the general public.

20 Q And "mission" probably is the wrong use of words there. Was that a goal,
21 though, of --

22 A Yes, that was a goal.

23 Q -- your group? The goal being to bolster and protect the public's
24 confidence in our elections?

25 A Understanding that there were adversaries that could target or that could

1 seek to undermine confidence in our elections, we then sought, as a goal, to boost
2 confidence in the American public's -- of the American public in our elections.

3 Q And do you think that goal was controversial within the CISA agency or the
4 Department of Homeland Security during the time you were there?

5 A Within CISA? Not that I -- not that I'm necessarily aware.

6 Q How about in the Department?

7 A Not that I recall. I mean --

8 Q Let me ask you another way.

9 A Yeah.

10 Q Did anyone from Department of Homeland Security ever tell you that
11 combating misinformation or seeking to boost the public's confidence in the election
12 system was inappropriate or outside your --

13 A Those are two different things, what you just said.

14 Q Okay.

15 A Right?

16 Q Yes.

17 A Countering misinformation and boosting the American public's confidence.

18 Q Okay.

19 A So, on the boosting Americans' confidence in the elections, absolutely not.

20 Q Okay.

21 A That was never a question. In fact, on election day, I had Chad Wolf at
22 DHS -- or at CISA headquarters talking to the American public. We had TV cameras
23 there, and he said that it was a secure election -- going to be a secure election, right?
24 So, you know, it wasn't just me. That was the nominee for the Secretary of
25 Homeland Security. Kirstjen Nielsen, actually confirmed Secretary of Homeland

1 Security, same thing. Kevin McAleenan, Acting, same thing.

2 So, you know, as far as I'm concerned, on the maintaining the confidence of the
3 American people in the election, that is part and parcel of the mission, right?

4 Q Now, you broke out the combating misinformation. So tell me about why
5 that might be different.

6 A So, again, combating mis- and disinformation is a nascent area within the
7 national security community. There are no, you know, clear national security strategies
8 around this. I think it's the -- I greatly respected and valued my advice from my chief
9 counsel and the DHS general counsel team. They were very clear on what was in play
10 and out of play. But I thought it was -- given how we understood the threats would
11 likely materialize, it became increasingly important, even probably more so than just
12 countering the technical threats, that the perception hacks, as they've been called, the
13 disinformation campaigns, would likely be the greatest threat to the 2020 election.

14 And, you know, this is not just about people on, you know, Twitter and Facebook
15 and whatever making false claims or whatever, but this was actually, as we, you know,
16 came to believe that it would be the -- sorry. It would actually be part of the techniques
17 used by, like, the Iranian actors, that they had, in fact, manipulated -- claimed that they
18 had manipulated the election when, in fact, they had not. But it would be their tactics,
19 because it's hard to rebut. It's hard to disprove a negative.

20 And so that was part of establishing, here are the security -- we never said, "No,
21 you didn't." We said, "Here are the security controls in place that would protect the
22 electoral process before, during, and after an election that would basically invalidate and
23 obviate any claims that they may make. And I have plenty of examples we can talk
24 about there.

25 Q Uh-huh. Okay.

1 You talked a little bit about -- I'm going to switch gears a little bit here. And I
2 might get to some of those examples in a minute.

3 A I'd love to talk about those examples.

4 Q Actually, why don't you --

5 A All right.

6 Q -- tell me about them now.

7 A Here we go.

8 Mr. Walden. How many days do we have?

9 Mr. Krebs. Jim -- I've talked about this. We've talked about this. All right.

10 So I think the biggest example here was, as I was in the seat at CISA, right,
11 Hammer Scorecard. So it's a claim that was repeated by some of the former President's
12 attorneys. Whether they were attorneys or not is unclear.

13 But, nonetheless, Hammer Scorecard -- Hammer is the CIA software that -- and
14 then Scorecard was the supercomputer -- supercomputer -- flip it around,
15 whatever -- that was developed by the CIA allegedly to manipulate elections of foreign
16 countries. The claim was that Hammer Scorecard had been flipped around and was
17 being used here in the United States to attack election tabulators.

18 And so our response here was, again, reverse-engineering the claim. So what's
19 the claim? The claim is that someone's using a software program to change tabulation
20 of the votes. Okay. So --

21 Q Stop for 1 second. When did that claim first arise in the context of the
22 2020 election? I think it might go back before then.

23 A I would have to go -- oh, yeah, it does, but I'd have to go back and look -- I
24 mean, honestly, I'd have to go back and look at my Twitter feed, but October, sometime
25 late October.

1 Q Before the election. That's --

2 A I believe so, but, you know, I don't want to say definitively here.

3 Q Okay.

4 A It could've been right around -- it was right about that time in November 3rd,
5 but maybe slightly earlier.

6 So, again -- so, okay, if the claim is that a bad guy comes in and adjusts the
7 tabulation, what is the material impact on an election that has robust safeguards before,
8 during, and after the election?

9 That ultimately is where we got to the point about paper being important.
10 Because if you have a paper record of how we all voted in this room and that is virtually
11 immutable as it moves through the process, it doesn't matter if there was a computer
12 that at some point counted all those things and then changed the outcome, because
13 you're also conducting audits on the other side.

14 So technology is used in elections to increase the accuracy and the efficiency of
15 the process, right? That said, election officials recognize -- this is a concept known as
16 software independence -- that you cannot have a computer or piece of software as a
17 single point of failure through the process.

18 And that's why in Georgia it was so critical that they did, in fact, move from the
19 DREs to a ballot-marking device that had a paper record. Because even if Hammer
20 Scorecard was correct and the first count of the votes was manipulated by a dead
21 Venezuelan dictator, as was claimed, the subsequent counting of the hard copies, the
22 paper ballots, showed consistency.

23 That software program could not have actually changed the physical paper ballot.
24 It could only change the digital tabulation. The recounts proved it did not, though.

25 And so our point was: Okay, this is the claim, this is what's circulating. Here, in

1 fact, though, are the security controls and the resilience measures in place.

2 And that is essentially how rumor control worked. We would identify the issue
3 or the theme that's being claimed, unpack it, reverse-engineer it, and then actually
4 provide -- not just say, "And, hey, listen to CISA," but "listen to these experts," the
5 national -- you know, the actual State laws, the Federal laws, whatever that is in place,
6 the best practice, on how that could not actually change the outcome of an election.

7 Q Okay.

8 Is there another example you want to share?

9 A Sharpiegate. So Sharpiegate is another example in Arizona where there
10 were claims that Sharpies were being intentionally passed out in certain voting locations,
11 and they would bleed through the ballot and bleed through and fill in a bubble or be read
12 as to fill in a bubble on the other side of the ballot if they're double-sided.

13 And, in fact, what -- so, first off, you know, what we would do there, we'd see
14 that, we'd see that it kind of makes national news or it circulates nationally, so we'd
15 contact our -- we either had our on-the-ground people or we would just work with the
16 secretaries of state offices. In that case, it was Katie Hobbs and her team. So this is
17 the team Matt Masterson would lead.

18 And he'd go talk to Katie and Katie's team and be like, hey, what's going on here?
19 She would say, well, here's the claim, and here's the actual -- the technical specifications
20 that we have here. And, no, a Sharpie cannot bleed through -- first off, Sharpies are
21 approved and have been tested for efficacy. But the second piece here is that, when
22 you look at the ballots, there is actually nothing on the other side. The way the ballots
23 were designed was that, even if it bled through, there was no scannable field on the other
24 side of the bleedthrough. So they were actually offset.

25 And so, again, that's the sort of information we can provide out and, again,

1 circulate out to the American public.

2 Q And was the -- again, I'm covering something that we've already talked a
3 little bit about. But, on that specific instance, no allegation of a foreign actor involved in
4 the distribution of Sharpies, right?

5 A Not that I recall.

6 Q Was there an allegation or a concern that foreign actors were spreading the
7 Sharpiegate --

8 A Yes.

9 Q -- claim?

10 A Absolutely.

11 Q And is that what you felt gave you the authority to respond in terms of
12 rumor control?

13 A I don't think we need -- I don't think we needed that assessment, no. I
14 mean, it was disinformation being, you know, associated with an election, with election
15 infrastructure, with election systems, and, you know, that, in and of itself,
16 election-infrastructure-related disinformation, was sufficient to engage.

17 Q So you didn't perceive that as a State issue that was outside the jurisdiction
18 of CISA, to try and address a false rumor about Sharpies?

19 A I think it certainly was a State issue, but, you know, it circulates much
20 broader than just Arizona, you know, the way the internet works, right? It's not
21 confined just to the State. It was, at that point, a national issue.

22 Q We've heard from DHS leadership, former leadership, that an allegation
23 that's sort of handled by the States would be outside the lane of CISA and, in fact, you
24 were going outside your lane by addressing issues such as Sharpiegate or other issues
25 regarding misinformation regarding the 2020 election.

1 A Certainly never told by anyone at DHS leadership that we were going outside
2 our lane that I recall.

3 Q Other -- I don't want to cut you off on other examples regarding rumor
4 control or misinformation.

5 A Oh, we talked about -- you know, we talked about the Hammer Scorecard,
6 we talked about Sharpiegate, I mean, we talked about secret ballots.

7 You know, a lot of the times -- you know, while there were cases where rumor
8 control was specifically to emerging claims, we had also done a significant amount of,
9 kind of, scenario development and threat modeling, so we had a prepopulated set of
10 rumor control entries prior to the election. And we'd actually send them up: You
11 know, here's what you might expect to hear prior to the election, here's what you'll hear
12 on election day, and here's what you'll hear after the election. But, as specific claims
13 came up, we were able to drop in and update new ones.

14 Q So, for example, I think you had a rumor control topic on dead people voting
15 and how that is not a thing and wouldn't be something that could move an election.

16 A I don't think that's how we characterized the response. I think --

17 Q That was a gross oversimplification of what was there.

18 A So, as we -- yes, there were claims about dead people voting that came
19 through. And, again, we don't move to disavow and say, that's not a thing, it doesn't
20 happen. The disinformation or the rumor control entry -- and this was coordinated with
21 State officials -- was, here are the security controls that are in use to identify dead people
22 and remove them from the voter rolls. And, you know, it's including coordination with
23 Social Security Office and, you know, the filing of the notice of a death and things like
24 that.

25 Q Likewise, I think there was a rumor control topic on changes in reported

1 unofficial results in the days and weeks following the election, sort of warning people that
2 that might be something that they would see and that they shouldn't be -- they shouldn't
3 take too much from that. Again, I'm mischaracterizing --

4 A No, this is --

5 Q -- a lot of the information that went into the rumor control, but was that a
6 topic for you guys?

7 A Yeah, we had --

8 Mr. Walden. Yeah, I'm sorry. I'm getting a little bit lost, so I apologize for this.
9 Maybe it's just me. But it seems to me that you're asking about two different things,
10 and I want to make sure you're that --

11 Mr. Krebs. Okay.

12 Mr. Walden. -- you're answering the right way -- the correct way.

13 One is whether or not the risk assessment for the issue was within his mandate.
14 The other one was whether the rumor control about the issue was within his mandate.
15 Do I understand your question correctly, or am I misunderstanding --

16 [REDACTED] Yeah. Sorry. It was probably a bad question. I'd sort of moved
17 off the mandate issue. Mr. Krebs was going through some examples and sort of racking
18 his brain, I felt, looking for them, and I'm giving him some -- I'm trying to jog his
19 memory --

20 Mr. Walden. Yeah.

21 [REDACTED] -- on things that I'd seen on the rumor control website.

22 Mr. Walden. Right. But examples of things that CISA actually dealt with from a
23 rumor control perspective is what --

24 [REDACTED] Yes.

25 Mr. Walden. Okay.

1

BY [REDACTED]

2

Q And is that true? Are these things that were dealt with, the things that I'm

3

mentioning?

4

A To the best of my recollection.

5

Q Okay.

6

Okay. Let me -- you've talked a lot about, sort of, your relationship with State

7

and local election officials. Was that an important part of CISA's work, to coordinate,

8

facilitate, assist State election officials in running their elections?

9

A To assist in securing their elections, to helping them conduct elections in a

10

secure manner, providing them security advice, technical cybersecurity assistance,

11

training, education, communications, support.

12

Q You talked earlier about the infrastructure and protecting that. How did

13

you work with State officials to make sure that their -- to help them ensure that their

14

equipment was safe and secure?

15

A We had a number of different offerings that we had. There's an entire

16

catalog. There's an election security catalog. It's not in here because it's thick. But

17

we would go out and conduct things like security and vulnerability assessments. We

18

could do red team. We could do fairly in-depth assessments of voter registration

19

database configurations.

20

We had a, what's known as cyber hygiene scan that they would sign up for and

21

we'd do a regular scan to see if anything touching the internet was mis- -- well, not

22

misconfigured, but running an old vulnerable version.

23

We developed in the summer before the election a product called -- or tool called

24

Crossfeed, which was a little bit more in-depth of assessing vulnerabilities of systems and

25

websites that are touching the internet. And then we would provide them reports and

1 technical assistance on how they might secure things.

2 And, you know, as they received money, we worked, through Federal grant
3 dollars, Help America Vote Act, we worked with the sector and government coordinating
4 councils to provide grant guidance on, you know, things they may want to invest in. And
5 that included things like hiring cybersecurity navigators, cyber navigators, that they could
6 put on staff and, you know, provide more technical -- you know, actual their
7 headcount -- cybersecurity technical advice.

8 Q Did all 50 States and the District of Columbia participate or coordinate with
9 you and work with you on infrastructure security?

10 A All 50 States participated in some way, some fashion. And it's typically
11 through the election infrastructure ISAC in all 50 States. We had thousands of
12 jurisdictions -- counties, cities, things like that.

13 In terms of, did all 50 States take a security capability? No. But that's not
14 dispositive, right? States have different investment levels. They have different organic
15 capabilities. They have different requirements. Some States, you know, didn't see a
16 need to, because they actually didn't have a lot of electronic or a lot of computer
17 infrastructure. They were fairly analogue or fairly remedial. And I think New
18 Hampshire is probably a good example of that.

19 Other States took every single service we offered, down to mandating it at the
20 State level all the way down to the county level. So Ohio, for instance, required every
21 single State to take a -- not just sign up for cyber hygiene but also participate in
22 a -- effectively it's a red team assessment. I can't remember what it's called at this
23 point.

24 Mr. Walden. I think you said State. You meant county, right?

25 Mr. Krebs. I'm sorry. At the county level. Every single county had to sign up,

1 not just for cyber hygiene but also down to the red team level.

2

BY [REDACTED]

3

Q Okay. What I'm trying to get to is whether you were able, based on the
4 work that you did with the States and the hygiene testing and otherwise, form any
5 conclusions, heading into the 2020 election, as to the States' preparedness from an
6 infrastructure security standpoint?

7

A So our assessment of the security posture of elections was that, to the
8 extent that we could get as many States, counties, jurisdictions, whatever you want to call
9 them, on paper, voter verifiable paper audit trails, that was ultimately the most resilient
10 posture that we could have, so that any sort of technical interference would be
11 moot -- mooted by, again, the immutable, auditable record of the paper ballots.

12

And --

13

Q Sorry. I didn't want to cut you off.

14

A So that was the -- that was one of the most significant pushes, was
15 encourage and get them the resources necessary to make that switch.

16

Q Understood.

17

A Yeah.

18

Q Were you also able to form any assessment of where the States stood in
19 terms of security against a direct hack, for example?

20

Mr. Walden. So, I'm sorry, you're asking a very broad question. I just want to
21 make sure that I'm clear so that he's clear. You're asking him for his opinion about all
22 the States, not whether there's a particular State that's an outlier or there were particular
23 States that were vulnerable?

24

[REDACTED] Fair question.

25

What I'm trying to get a sense of is whether you had the ability to make an

1 assessment --

2 Mr. Krebs. Right.

3 [REDACTED] -- regarding all the States. I'm not looking for the assessment yet,
4 but --

5 Mr. Krebs. Right.

6 [REDACTED] -- I can envision the answer that, well, you know, we never really got
7 into New Hampshire, so I can't tell you about New Hampshire.

8 But, you know, were you able to form impressions -- yeah, go ahead, John.

9 Mr. Luce. I guess one thing I was trying to understand is if you're asking, like, if
10 the Department established that or if you're asking, like, for his personal assessment.

11 At some points, it's getting a little bit confusing as to whether you're asking, like,
12 his opinion, like, almost like an expert-type opinion on something, or whether we're
13 getting to, like, what the Department knew or thought at the time.

14 So I just wanted to make that point and try and clarify for the record where we
15 are.

16 [REDACTED] Great. Thank you, John. I will try and clarify that.

17

BY [REDACTED]

18 Q It appears from your prior answer that -- or answers -- that it was critical,
19 from CISA's perspective, to try and move as many of the jurisdictions as possible to paper
20 ballots for all the reasons that you've said.

21 A Uh-huh.

22 Q Am I right on that?

23 A That was -- yes.

24 Q Okay.

25 I know it was also, based on your answers earlier, a goal of CISA to assist States in

1 ensuring that their -- not just States, but the jurisdictions -- that their equipment was safe
2 and secure, right?

3 A Right.

4 Q And you talked about hygiene tests and other opportunities that you
5 presented to these various jurisdictions they could avail themselves of or not to sort of
6 test the equipment and make sure that they were as secure as they could be from an
7 infrastructure standpoint, correct?

8 A So, to step back, our job here was to build relationships with State and local
9 election officials who were, under the Constitution, as delegated by their State
10 legislatures, responsible for administering elections. We were there to help them do so
11 in a secure way.

12 So we'd build the relationship; we'd provide the resources that they need,
13 understanding that they have other resources. A lot of other States, counties, had, for
14 instance, FireEye and CrowdStrike and other things like that. If we determined or they
15 asked, "Hey, we don't have this capability," we could provide that.

16 Now, am I going to say right now that I have a full understanding of all 50 States
17 and whether they were an A or a B or a C or an F? No. That's not -- you know, I don't
18 have that understanding right now today.

19 So, all of that said, we also -- we're in the risk management business. So
20 100 percent security was never the objective here. The objective was a resilient election
21 so that, even if a technical attack by the Russians, by the Iranians, was successful and they
22 could infiltrate a voter registration database or whatever, it wouldn't matter, because,
23 again, the security safeguards in place would protect the integrity of the vote, the ballot,
24 all the way through the certification process. We had the utmost confidence in that
25 workflow.

1 Q Understood. Understood. And I'm going to --

2 A I know -- all right.

3 Q -- go a little more -- I'm going to push you a little more just to see if I can get
4 an estimate from you on this. But what I'm interested in understanding is, from a CISA
5 perspective, not Chris Krebs as an individual, whether your level of penetration, level of
6 cooperation, from the various jurisdictions with respect to this, these testing measures
7 that you offered, sort of how broad that reach was, to the point where you could say, for
8 example, in 50 percent -- I'd say, you know, in half the States in the country, you know,
9 we worked with them and we're pretty confident, based on the work that we did, that
10 their systems were not impervious but pretty secure against a direct hack, but a lot of the
11 States didn't avail themselves of that, so I don't have visibility.

12 I mean, that's the kind of assessment I'm trying to get in terms of what CISA's
13 visibility was or confidence level with respect to the security of the infrastructure in these
14 States.

15 Mr. Walden. Yeah. And I don't want --

16 [REDACTED] And if this is impossible, then just tell me, and I'll move on.

17 Mr. Walden. Yeah, I don't want to be a stick in the mud here, but maybe it'd be
18 a good time to take a little bit of a break. Are you talking about while he was there
19 before the 2020 election?

20 [REDACTED] Yes.

21 Mr. Walden. Okay.

22 [REDACTED] Do you want to take a break? We can. Talk about it?

23 Mr. Walden. Yeah, why don't you let us talk about it.

24 [REDACTED] That's fine.

25 Mr. Walden. Okay.

1 [REDACTED] That's fine.

2 Mr. Walden. By the way, is there any place around here that has coffee, like,
3 immediate to this room?

4 [REDACTED] There's a place in the basement.

5 Mr. Walden. Oh, no, no.

6 [REDACTED] But it's not --

7 Mr. Walden. It's not, like, there.

8 [REDACTED] No, unfortunately.

9 [REDACTED] [REDACTED], can you click this over there --

10 [REDACTED] Yeah.

11 [REDACTED] -- if you remember how to do that?

12 [REDACTED] Okay. We're going to go off the record now.

13 [Recess.]

14 [REDACTED] Okay. We're back on the record with Mr. Krebs.

15 BY [REDACTED]

16 Q So, Mr. Krebs, we've talked a lot about efforts made by the Department, or
17 the Agency -- excuse me -- heading into the 2020 election. I want to talk a little bit now
18 about your perceptions and understanding of how things went from a security standpoint
19 with respect to the 2020 election.

20 Do you -- let me ask this way. We've talked about the various measures that
21 CISA took and the work it did with State and local election officials in attempting to
22 secure the election. Do you have a view as to whether your efforts were successful in
23 terms of preventing cyber intrusion in connection with the 2020 election?

24 A So I believe three things. First is that we improved the security of the
25 systems across the country in general, through providing technical assistance and

1 services, tools, education, and awareness. So that's point one.

2 Point two is, I think we, more importantly, helped to improve the resilience of the
3 system where, even if there was a successful attack, that it would've not fundamentally
4 had an impact. Paper, again, resilience, the systems, that was the ultimate objective
5 there.

6 And I think, third, and probably, you know, most significantly as we came around
7 to understand, is that I don't ultimately believe that it was the objective of any adversary
8 to change a single vote in the election. I think their objectives were more to sow chaos
9 and undermine confidence in the process.

10 Q Are you able to form any conclusions as to whether there was a cyber
11 intrusion in connection with the 2020 election?

12 A Yes. In fact, we released alerts on these things throughout. There were
13 both Russian and Iranian actors that were able to gain access to election-adjacent
14 systems. The Iranians, in one case, I think, had access to a voter registration database.
15 But we're not aware of any instance where they were in a system that would've been
16 directly connected or, you know, involved in casting, counting, certifying of votes.

17 Q You're speaking specifically of the Russians in that last answer?

18 A Both. Anyone, any actor --

19 Q Okay.

20 A -- that would've been able to change a vote or change the tabulation of a
21 vote.

22 And there are CISA and FBI alerts on both Russian and Iranian actors. I think
23 those are sequentially dated, like, the 27th and 28th of October, something like that.

24 Q And with the Russians, I think the public information was that they gained
25 access to voting records or some sort of voting registration records?

1 A The -- again, this is over a year -- they had access in a county in the Midwest
2 and a county on the Pacific Coast, at a county level, in a voting office, but it was
3 effectively derivative work product. So I would think about it more along the lines of,
4 they had access to a merge mail file for voter -- it effectively would be like sending a voter
5 postcard, like, "Remember, here's your voting location," that sort of thing.

6 Q And had there been public reporting of some sort of intrusion by the Iranians
7 before the election?

8 A That was associated with the Proud Boys campaign. I would think about
9 this less of a single action, of a set of emails, but more of a coordinated campaign. You
10 know, I'd point you again to the joint CISA-FBI alert that talked about how they had access
11 into a State level -- again, I'd have to go back and look at the alert of exactly what the
12 system it was. But, again, it had nothing to do with the actual process of casting,
13 counting, or certifying the vote.

14 Q Have you seen any evidence of cyber interference along the lines of casting,
15 counting the votes, with respect to the 2020 election?

16 A No.

17 Q Have you heard any reputable scientist or electronic voting expert conclude
18 that there was cyber interference or manipulation of votes with respect to the casting or
19 counting of votes in the 2020 election?

20 A No.

21 Q In your binder, at exhibit 2, there's a November 16, 2020, statement --

22 A Yes.

23 Q -- signed by 59 -- not signed but sort of electronically or listed as having been
24 signed by 59 different specialists in election security.

25 Have you seen this document before?

1 A I have.

2 Q Okay. Do you know some of the people who are listed on the second and
3 third pages of this document?

4 A I do. I know a number of them.

5 Q Okay. And is your understanding that these are, indeed, experts in the area
6 of election security?

7 A These are the experts in election security and computer security in the
8 United States.

9 Q Did you see this statement at the time that it was issued?

10 A I did.

11 Q Is there anything in it that you disagree with?

12 A Nothing at all.

13 Q Did you play any part in the preparation of this document?

14 A Preparation, no.

15 Q How about distribution?

16 A I tweeted about it.

17 Q Okay.

18 A In fact, I quoted a line.

19 Q Do you remember what line that was?

20 A Yes. I think the tweet was something along the lines of, you know: 59
21 election security experts all agree, in every case of which we are aware, these claims
22 either have been unsubstantiated or technically incoherent.

23 Mr. Walden. The first page in the fifth paragraph.

24 Mr. Krebs. Yeah. Sorry. Halfway through. Starts with "however."

25 BY [REDACTED]

1 Q Got it. Thank you.

2 Let me step back again to before the election. Were you keeping others within
3 the government apprised of CISA's efforts to help secure the 2020 election?

4 A Within the Department?

5 Q Within the U.S. Government.

6 A Oh, absolutely.

7 Q Were there interagency meetings on those topics?

8 A There were frequent interagency meetings.

9 Q Which -- and, again, I'm going to tread carefully here. I certainly don't want
10 to get into any classified information, but let's just start with who -- if you can say, which
11 agencies participated in the frequent briefings or --

12 A Okay.

13 Q Maybe a better way to ask that is: Which agencies did you brief on election
14 security efforts leading up to the 2020 election?

15 A So I think there was -- let me put a real quick, kind of, framing around those
16 meetings. There were separate meetings through separate channels.

17 So there's a National Security Council process that's run by an SPM-4 (ph). And
18 that starts with a -- whatever -- a PCC, so a policy coordinating committee, or a sub-PCC,
19 that works its way up to a deputies committee meeting and then goes to a principals
20 committee meeting.

21 So, at the PCC level, it's typically assistant secretary level -- supposed to be, but it's
22 probably a little bit below that. Deputies committee meeting is either deputy
23 secretaries of departments or, in some cases, agency heads that are sub-department.
24 And at the principals committee meeting, that is as established in the National Security
25 Act, and that tends to be agency heads.

1 So that is the formal process that's run by the White House through the National
2 Security Council.

3 There is a separate coordinating process from an operational agency perspective
4 that was -- and you had in some of the production that I saw, some of the calendar
5 invitations that talked about principals commit- -- or principals -- I don't know if you have
6 it in here.

7 Q I don't think it's in the binder.

8 A So it was principals SVTC.

9 I don't know if I see it in here, but --

10 Q Yeah.

11 A -- it was definitely in some of the stuff that I saw.

12 So, anyway, in the principals SVTCs, those were coordinated or run by the Director
13 of National Intelligence, ODNI.

14 Mr. Walden. Can we just stop --

15 Mr. Krebs. Yeah.

16 Mr. Walden. SVTC?

17 Mr. Krebs. SVTC, secure video teleconference.

18 Mr. Walden. Thank you.

19 Mr. Krebs. Didn't you work at DOJ?

20 Mr. Walden. Yeah, I did. I just like to have a clean record.

21 Mr. Krebs. Right.

22 And those would happen -- again, I'd have to refresh my memory, but those
23 started in 2019 to 2020, early, and then ran through maybe about the summer or so, or
24 the late summer. And those were -- so the principals committee -- or the, sorry, the
25 principal SVTCs were run by whoever was leading the Office of the Director of National

1 Intelligence.

2 Now, when Rick Grenell came in, those meetings dropped off. We didn't do
3 them anymore. Nor did we do the deputies level, which was -- so the principals were
4 about every month, and the deputies meetings were about every other week, so every
5 2 weeks.

6 And so those started with, at the deputies level, Coats and Sue Gordon. It really,
7 I think -- yeah, it started at the tail end of Coats' and Sue Gordon's tenure, and then
8 Joe Maguire and Andrew Hallman. And then, when they left in late February, which is
9 about when they were shown the exit, and Grenell and Kash Patel came in, we didn't -- I
10 don't recall ever being in a meeting with Rick Grenell or Kash Patel about election security
11 stuff.

12 So that was -- but they were still happening at kind of the lower staff level. And
13 Shelby Pierson was leading those discussions on behalf of the DNI with Bill Evanina, who
14 had been tapped at the tail end of the -- you know, in the interregnum, basically, after
15 Coats and Maguire, that period.

16 Q And, just to stop you there, in the context of these DNI-type briefings, were
17 you sharing CISA's efforts on election security and what the agency was doing?

18 A Absolutely. We were sharing -- I mean, we had a very prominent role in
19 updating what we were doing at the State level, the sorts of meetings that were
20 happening. There was a big roll-out and a communication strategy. There were public
21 events. You know, this was at the level of -- you know, in February of 2020, I'm going to
22 San Francisco to keynote the RSA conference, the largest cybersecurity conference.
23 Like, that's the sort of detail, as well as, well, we've got a tabletop exercise, we have this
24 sort of meeting.

25 But it was not just those were updated in the meetings; there was a tracker that

1 was maintained at the staff level across the agencies, as well back up to the National
2 Security Council through the PCC. I think they actually called it an IPC, but it doesn't
3 matter.

4 So that was that operational coordination piece that, over time, as we got closer
5 to the election, I think the responsibility of leading the regular engagement shifted from
6 this DNI-driven effort to a National Security Council coordinated effort at the sub-PCC
7 level. And so those were run by -- the name escapes me right now, but it was a -- I
8 believe it was a DHS detailee to the National Security Council Resilience Directorate,
9 which, at the time, the senior director was Brian Cavanaugh.

10 Q Okay.

11 And it sounds like, either through the briefings or the tracker or other mechanisms
12 or maybe just, you know, operational collaboration, you were keeping other agencies in
13 the executive branch pretty well informed as to the measures and the initiatives that CISA
14 was undertaking.

15 A Yes. And they shared back with us. And it was DNI, FBI, Cyber Command,
16 Department of Defense, the CIA, and anyone else in the intelligence community that
17 wanted to share. Those were generally the players in that DNI-led effort.

18 And then, as that transitioned over to National Security Council, it was a similar
19 cast of characters.

20 Q How about the White House directly? Were you keeping the White House,
21 through a liaison or otherwise, apprised of the initiatives and measures that you had
22 underway, so tabletop exercises that you've talked about, rumor control, things of that
23 nature?

24 A My -- because I did not -- you know, my team, staff, worked directly with the
25 National Security Council through the PCC process, and I was not involved in those

1 conversations. They were staff-level, weekly. I think it was, like, every Tuesday, they
2 would have meetings with the White House. But those conversations had all the
3 information. And there were, as far as I know, White House representatives, you know,
4 politicals, that had access to that information.

5 Did I directly update the White House? No.

6 Q Did you ever get feedback, either directly or through your staff, about
7 concerns that the White House had about efforts that CISA was undertaking in the
8 election security area before the election?

9 A So the concerns that I heard -- again, nothing came directly to me from the
10 White House. In point of fact, I made it clear that if there were concerns they had to
11 come to me. But that there were some concerns through the, kind of, the political
12 apparatus, and whether it was from the White House or the White House liaison at DHS,
13 but there were concerns about a product we released in June or July of 2020 about
14 security -- oh, a risk assessment of mail-in voting and the security controls that were in
15 place.

16 Q What did you understand the concern to be?

17 A So, as it was fed back up to me from staff is, why are we providing guidance
18 on whether a form of voting that the President has said is insecure -- why are we saying
19 that here are security controls for it?

20 And my response to that was, if someone has a concern with that product, they
21 will come talk to me about it and we'll have a discussion about whether it stays up or
22 stays down. Nobody ever came to me.

23 Q So you heard that concerns had been raised. They were described to you.
24 But you didn't take any action with respect to those, and you never heard directly from
25 the people who were concerned. Is that --

1 A That is accurate.

2 Q -- fair? Okay.

3 A I was -- you know, I had the -- as the Senate-confirmed Director of the
4 Agency, it was my responsibility to make decisions of what was up and what was down.
5 And I was not going to, you know, put that decision authority in subordinates' hands.
6 That was mine.

7 Q Do you know that -- I'm going to ask the question this way. Did you know
8 that, in fact, some information regarding mail-in voting was taken down or redirected?

9 A After the fact, I was informed that stuff may have been taken down, but it
10 was, as I understand, put back up.

11 Q Other than this concern that got to you indirectly regarding the
12 mail-in-voting directive, any other concerns that were raised with you --

13 A Let me add one more little addendum to that last statement.

14 So I made it completely clear that I was the one in the Agency that was making
15 decisions on what stayed up and what stayed down -- or what stayed up or what came
16 down. And so I think, as that percolated through, perhaps that's what led to, oh, this
17 goes back up.

18 Q Okay.

19 Other than the concern that got back to you regarding mail-in voting, any other
20 concerns ever brought to your attention, either directly or through staff, that the White
21 House had about election security efforts being undertaken prior to the election?

22 A Not that I recall.

23 Q Or any concerns about statements that CISA was making publicly in
24 anticipation of the election?

25 A Not that I recall. In fact, many of our statements were encouraged by the

1 White House, like encouraging voters to be patient, that results may take time to come in
2 and the official results are not until December.

3 Q Were there other aspects of CISA's work that you were encouraged by the
4 White House to more broadly publicize?

5 A In fact, we had a campaign known as "Be a 3P Voter." Be prepared, you
6 know, because things are changing with COVID, know where you're supposed to vote.

7 The second is be a participating voter, because there were a lot of concerns about
8 elderly voters or elderly election volunteers, because of COVID, not being able to
9 volunteer. So they wanted to get people to volunteer to work polls.

10 And the third is be a patient voter, purely because the increase in mail-in voting
11 would take a longer lead time and it would take more time to work through.

12 And so that point specifically, be a patient voter, was briefed out numerous times
13 in White House meetings and with full endorsement to continue pushing that message.

14 Q I think I've heard somewhere that, at one point, the President suggested to
15 someone who worked for you that there should be more publicity of the successes that
16 were --

17 A Yes.

18 Q -- generally of the successes of the Agency. Correct?

19 A I believe that was expressed to Matt Masterson in the Oval Office on Friday,
20 February -- what was that -- 14th? I was in Munich, so I don't know. But --

21 Q And specifically with respect to the positive trend that you've talked about
22 towards paper ballots, correct?

23 A The President, in his own public statements, encouraged paper, yes.

24 Q But was there a request that CISA be more outspoken about this
25 accomplishment, with respect to the encouraging and facilitating the move to paper

1 around the country?

2 A What are you -- are you asking that we get out there and talk -- that we were
3 to get out there and talk about how we've increased the resilience, or how the President
4 was responsible for increasing paper?

5 Q Either.

6 A So, you know, that -- I was not in that meeting. Matt Masterson was. It
7 was not a surprise to us; he had been a constant supporter of paper ballots. And that
8 message kind of, I think, trickled through the White House, that, you know, as a
9 government, we need to get out there and talk about our successes in making the
10 election secure. And we did that.

11 Q So you had a specific, very specific, recollection in mind in terms of the date,
12 time, and place and individuals. Are there other examples of that that you're aware of
13 where word got back that the President wanted you to promote or tout a particular
14 success of the Agency?

15 Mr. Krebs. Do you have any concerns?

16 [REDACTED] I don't want to --

17 Mr. Luce. Can we just have a quick --

18 [REDACTED] Yeah. Let's go off the record.

19 [Recess.]

1

2 [12:13 p.m.]

3

BY [REDACTED]

4

Q Okay. There may have been a question pending, but I'll withdraw it. Let's

5

move on.

6

A All right.

7

Q Mr. Krebs, in your last -- one of your recent answers, you mentioned sort of

8

issues raised by the pandemic and COVID concerns. Was that -- did the pandemic in

9

the -- leading up to the November 2020 election create certain challenges, from an

10

election standpoint?

11

A Yes, there were a number of challenges introduced. One, you had delays in

12

holding of primaries. You had, you know, certain safety measures introduced at polling

13

locations, like baffles, masks, pencils, separation 6 feet, things like that. There were

14

concerns about whether COVID could be transmitted on paper ballots and things of that

15

nature.

16

And so one of the -- again, consistent with that kind of all-hazards mission of CISA

17

in the critical infrastructure protection and resilience space, we early on both worked

18

with our State and local election officials and the HHS and CDC, so that they could provide

19

election-specific guidance to election officials, so COVID election-related specific

20

guidance.

21

We also connected State and local election officials with the post office to talk

22

about some of the security -- or the concerns about potential COVID impact on the

23

election process. And, I mean, I think that's generally it in the spring.

24

Q Are you familiar with the term "swimlane documents"?

25

A Now that I -- that you mention it, I haven't heard -- I haven't heard that term

1 in a while, but yes.

2 Q What were swimlane documents?

3 A I -- those documents, as I recall, were for staff to have a clear understanding
4 between -- actually, I'm going to -- I don't believe I have a recollection that I would
5 be -- feel comfortable, you know, recalling exactly what that document was, because I
6 don't remember if it was for specifically the election side or the interagency side.

7 Q Okay. Prior to the election, did you become aware of any -- what -- and
8 this is a Chris Krebs personally question. Did you become aware of any information that
9 you would consider misinformation regarding the upcoming election that was being
10 disseminated by the White House, by the President or his spokespeople?

11 A What's the timeframe again?

12 Q Leading up to the election, at some time prior to November 3rd.

13 A I think generally the -- the mail-in ballots would be rife for foreign
14 interference, that foreign actors could mail in a bunch of fake mail-in ballots. I mean,
15 that's just one example.

16 Q There was a press conference that I'm recalling, I can't give you the date,
17 where an issue of ballots being found in a river in Wisconsin came up. I think the
18 President might have said that. Don't hold me to it. But I know his spokesperson
19 addressed that issue prior to the election. Do you remember that?

20 A I recall the instance. I don't recall exactly what -- when that was or what
21 we said about it, if anything.

22 Q Okay. Well, the last part is what I was most interested in, is whether there
23 were any efforts within CISA to address claims that had been made by the President
24 regarding the upcoming election that people within your agency might have believed to
25 be false?

1 A Again, when you go to the philosophy of rumor control, it was to identify
2 themes. It was not rebutting specific examples or statements by any individual.

3 Q We've seen some documents that were produced by DHS relating to efforts
4 to connect with social media platforms, Twitter, for example, to working with State and
5 local officials to try to address claims that were being made on Twitter that were false.

6 A Uh-huh.

7 Q Are you familiar generally with that initiative?

8 A I think generally, yes. And I gave an example of the 2018 election, at least,
9 how we were able to connect I think it was Ohio with one of the platforms.

10 Q And it seemed as if that was a fairly robust -- I was going to say operation.
11 That's probably too strong a word. But there was a fairly -- it looked to be, from the
12 documents I've seen, a fairly well-coordinated effort to put State officials in touch with
13 the social media platforms and try to provide the information necessary to address what
14 were false claims in their respective jurisdictions.

15 A I think certainly the efforts to make those connections was a priority. We
16 had frequent -- I think it was monthly -- at least monthly -- I think monthly, let me put it
17 that way -- meetings between interagency partners, so FBI, DNI, and CISA, with
18 representatives from the social media platforms. And we sometimes did those out in
19 California. You know, I would attend every now and then some of those meetings.

20 Now, State and local partners were not there. This was just making sure the
21 Federal Government and the social media platforms were connected and were sharing
22 kind of our understanding of how things were playing out, what our concerns were.

23 Q Were you generally -- are you aware of the general process if, for example, a
24 tweet was posted about a particular claim in a particular State, what the process was to
25 try to -- that might lead to either addressing it or deplatforming the person who had --

1 A No.

2 Q -- made the tweet?

3 A No. I was not -- I didn't have kind of visibility into the mechanics at that
4 level.

5 Q Okay. Do you know whether CISA played any role, for example, in helping
6 secretaries of state formulate a rumor control type of response to those -- those
7 instances?

8 A Meaning their own responses at the State level to -- I -- I don't know for
9 certain. I wouldn't be surprised, but I don't know for certain.

10 Q I mean, I can see that those types of responses -- when I say types of
11 responses, there were responses coming out of various State -- from various State
12 election officials akin to what you've described with rumor control.

13 A Right.

14 Q So not necessarily debunking, but sort of promoting sort of true facts that
15 the public should be aware of. And I'm wondering whether CISA played a part in that or
16 that was just sort of training and they would sort of do their own thing.

17 A I don't believe -- I don't recall any specific training to States in advance of
18 elections on, you know, how to counter. Rumor control kind of came up more
19 organically than that.

20 I do recall -- I can't give you a specific here, but if there was a State-specific claim
21 that I would ask or I would be asked -- it's in the bits here -- about, hey, this -- I'm seeing
22 reports of this, what -- what's going on?

23 And so what we would tend to do is ask the State officials, say, hey, what's
24 happening in this issue, is there anything you can share, do you have a statement? And
25 then I could take that statement and send it to the Acting Secretary or the White House.

1 We would send it to the White House.

2 Q Okay. Did you ever interact with a person named Josh Whitehouse?

3 A Yeah. He was the White House liaison before he went -- for DHS before he
4 went to DOD, yes.

5 Q Did you have personal interactions with him?

6 A I talked to him a handful of times. He interviewed me, and I tried to get
7 him to not take personnel action against some of my employees.

8 Q He interviewed you in what context?

9 A So in the press they've been dubbed loyalty tests, but he -- in
10 the -- throughout the course of 2020, as I understand it, at various departments the
11 White House liaisons were to interview staff to, you know, in part say, hey, what do you
12 want to do next term. But, you know, there were other cases where I think they were
13 asking about operational issues and, you know, what your coworkers are like.

14 Q What types of questions were you asked?

15 A I don't recall other than, you know, it was a fairly -- so I don't
16 think -- actually, Josh was not in my interview. It was Troop something that
17 was -- Cooper something, I don't know, that was -- he conducted the interview. And it
18 was background questions, you know, what do you want to do, and things like that. It
19 was --

20 Q So with Mr. Whitehouse, did you ever have discussions with Mr.
21 Whitehouse in which he expressed concerns to you about any aspect of what CISA was
22 doing?

23 A Not that I recall about any of our actions. He had concerns about people
24 that worked for CISA as political. I don't know if I'm -- is this in play?

25 Mr. Luce. I think at this level --

1 Mr. Krebs. Okay, okay.

2 BY [REDACTED]

3 Q Concerns about people who worked under you?

4 A Yes.

5 Q And their loyalty to the President?

6 A I think it was -- that's, you know, one way to characterize it. I think it was
7 just general -- yes, loyalty to the administration.

8 Q Did anyone -- prior to the election, did anyone from DHS leadership ever tell
9 you that your job was in jeopardy?

10 A It wasn't so much that I recall specific instances. It was just that there
11 was -- so just stepping back, and you see it here in this. I'm holding the Krebs strategy
12 that was posted publicly on Twitter by Jonathan Karl.

13 You can see in here that there's a line that says -- you know, assuming this is, in
14 fact, real, it's consistent with my understanding of how the White House personnel office
15 under John McEntee viewed -- "Maintains a close and personal relationship with Nielsen."
16 So there's just this broader theme that we were part of the John Kelly-Nielsen cabal, and
17 that was a bad thing.

18 So I was aware that there was, you know, some skepticism of my loyalty to the
19 President.

20 Q How did you become aware of that? You didn't have this document, the
21 one that you just --

22 A I didn't have that document. I think -- again, I can't tell you specific people.
23 It was just kind of the whisper net. I knew that, for instance, that they wanted to fire
24 Bryan Ware, and they did fire Bryan Ware.

25 Q "They" being who?

1 A The PPO, White House. Not Josh Whitehouse, but he was the vessel for
2 that, but it was the Presidential Personnel Office. In fact, they tried to fire him the
3 summer of 2020, and then I was able to convince them that it would be in the President's
4 best interest to keep him on until after the election.

5 Q But with respect to you personally, you had a sense that you maybe were
6 perceived as less than completely loyal to the President?

7 A I think it was -- again, I can't point to any specific conversation or person, but
8 it was, you know, the profile. Nielsen, Bush administration, you know, didn't serve on
9 the campaign or anything like that. And, you know, so that kind of led up to it. And,
10 again, I think there were comments made over periods of time, but I can't say it was any
11 specific person.

12 Q Were you ever told that there were -- other than -- we talked about the
13 mail-in voting piece. I'm not even sure this would fall into that category, but were you
14 ever told that there were concerns at the White House about how you were running the
15 agency?

16 A Never.

17 Q Were there any specific measures or actions that you took that you received
18 feedback that was -- that those actions were not well received at the White House, other
19 than what you mentioned before about the mail-in voting guidance?

20 A So after Claire Grady left, which was 2018 -- what was that, March of 2018?

21 Q Who is Claire Grady?

22 A Claire Grady was the Acting Deputy Secretary. She was the
23 Senate-confirmed Under Secretary for Management who was -- who served as Kirstjen
24 Nielsen's deputy.

25 After Claire left, I didn't have any formal performance evaluations. So I went,

1 you know, 2-plus years, 2 and a half years without a formal performance evaluation.

2 And there was no other mechanism that I received any feedback on my job performance,
3 how I was managing the agency, other than laud, you know, very confident feedback, in
4 fact, from Kevin McAleenan, from Chad Wolf, that, you know, we were doing -- you know,
5 we're -- they don't have to worry about us, basically, because we're running a tight ship.

6 Q So -- I'm not just confining this to sort of a formal job evaluation, but did
7 Mr. Wolf ever tell you on any particular issue, you know, there are concerns about how
8 you've handled that issue, concerns at the White House?

9 A What issue?

10 Q On any issue.

11 A I am not -- I don't recall any specific conversation I had with Chad that I could
12 pin back, point back to. I think there was, again, a general sense that, you know, I
13 wasn't necessarily perceived very positively in the new PPO.

14 Q Based on your background profile and former sort of affiliations, but not
15 necessarily based on particular work you had done or decisions you had made, as you
16 understood it?

17 A That's as I understood it, right. I just don't think there was necessarily a
18 science to any of this. I think it was all very vague and --

19 Q Okay. And I'm not asking you to sort of read what other people were
20 thinking or that. I'm focused here on whether you were ever told specifically there is a
21 concern about how you handled this or that situation?

22 A I was never -- as far as I can recall, never counseled on any specific issue or
23 decision I made. I had a general sense, though, that I was not on -- viewed as being on
24 the team.

25 Q And I asked specifically about Mr. Wolf. I want to also ask specifically

1 about Mr. Cuccinelli. Did he ever share with you that there were concerns about how
2 you were handling any particular issue at CISA?

3 A Any particular issue? No.

4 Q Or concerns that the White House is not happy with the way you handled a
5 particular issue?

6 A On any particular issue, no.

7 Q How about the general concept -- this is from Mr. Cuccinelli -- the general
8 idea that you were getting outside of your lane in some actions you were taking on behalf
9 of CISA?

10 A I was never informed or told or counseled or advised, to my recollection,
11 that I was getting outside of my lane.

12 Q I want to turn my attention now to election sort of -- this is sort of leading up
13 to the election. Now I want to talk about election day a little bit.

14 What was CISA's role on election day?

15 A We hosted at -- at CISA headquarters in Arlington the -- kind of the war
16 room. In fact, we had -- so that was November 3rd, Tuesday. I think we spun it up.
17 The virtual room was up and running the week before, I think Thursday -- no, maybe
18 actually like Tuesday, Wednesday, Thursday before. We had people in the office
19 physically, even in the middle of COVID but in COVID safe protocols, on I think starting
20 Monday, maybe even Sunday night. And that ran through Wednesday.

21 We kept the virtual where virtually I think every State. We may have had like 47
22 or 48 States dial in throughout, but that went on. That was like a week or two in
23 advance to a week or two after, almost I think through certification.

24 But on election day, we had operational representatives from the FBI, the
25 intelligence community, State and local election officials. I think we had representatives

1 from social media companies, and we had representatives from election equipment
2 vendors. Cuccinelli was there. So Chad Wolf was there in the morning. We did a
3 press conference. There was press there. Cuccinelli came in the afternoon.

4 Throughout the day, I think every 3 or 4 hours, we did press calls where national
5 media would call in and ask us questions. But it was, as I said at the time, just another
6 Tuesday on the internet.

7 Q What was the role of -- you had this structure set up. Talked about sort of
8 who was there. What were you -- what were your -- what do you perceive as your role
9 that day or night?

10 A So -- all right. Generally, we were coordinating massive amounts of
11 information as they were flowing across the country. So, you know, hey, there's an
12 issue in whatever county, Georgia, what's going on there? It's hitting national news.

13 So it's basically like a watch function. It's like, hey, we're seeing reports that this
14 thing happened. And then we make a call down to the State and say, hey, getting
15 reports here, what's happening? Oh, a backhoe cut a fiber line going into an election
16 precinct and they've lost internet connectivity. Okay, all right, let us know when it's
17 back up.

18 Q And the goal of that -- the local jurisdiction is obviously aware of it, that's
19 who you're getting your information from. They're dealing with it. What's
20 CISA's -- why is it important that CISA be advised of --

21 Mr. Krebs. Hanging in there?

22 Mr. Walden. Yeah, yeah. I'm going to need a break for a minute to just walk
23 down the hallway. I apologize. I don't mean to -- finish this line of questioning. I just
24 need to walk for a minute.

25 Mr. Krebs. Decision support, in part, to leadership at DHS or at the White House.

1 Second is operational, you know, informing operations if there's anything
2 suspicious.

3 You know, what we really wanted was that if any State or local government saw
4 something suspicious happening, that they would immediately inform us.

5 And so there was a case where a State -- it's in your tracker that I was provided,
6 one of the exhibits that had the kind of the day of. And I think this was one that Melika
7 passed to Cuccinelli that -- anyway, it's a tracker. It's an Excel spreadsheet.

8 And there was a State, Delaware observed an unknown actor trying to exploit an
9 Oracle database vulnerability that they had had patched. So what we were able to do is
10 Delaware let us know. We said, that's interesting. But because we were integrated
11 with the FBI and the intelligence community and others, we could actually say, hey,
12 guys -- so it wasn't just for our benefit, like I said, decision support. We were able to
13 share it with our operational partners for them to go do whatever they need to do.

14 So it was a functional operational watch cell, also coordinating situational
15 awareness, coordinating action. And that was -- and that was the day.

16 [REDACTED] Let's go off the record.

17 [Recess.]

18 [REDACTED] Okay. We're back on the record.

19 BY [REDACTED]

20 Q Mr. Krebs, did you make any public statements -- and this is you
21 personally -- make any public statements regarding election security in the days following
22 the election?

23 A While I was still a CISA employee or after?

24 Q Yes, in the days immediately following the election.

25 A So on the -- obviously, November 12th was the joint statement, the GCC-SCC

1 statement.

2 Q Let me stop you right there. I'm talking about before that. On the 3rd,
3 4th, 5th, were you making -- did you make any public statement?

4 A I think -- yeah, I think even on election day, as I just -- I just said, you know,
5 we've said that it was just another Tuesday on the internet. So we didn't see any
6 activity on that Tuesday on the immediate aftermath that would have suggested there
7 was any sort of security issue associated with the election.

8 Q Just another Tuesday, that was a tweet from you?

9 A No. I said that on the press call that was then quoted in an article. I don't
10 recall exactly -- I don't remember who exactly quoted it, but it was to a -- we did all those
11 calls on background. So it didn't get attributed to me, but it was me.

12 Q How about Mr. Wolf, was he -- did he make statements either on election
13 night or in the immediate days following?

14 A As I recall, you know, that morning, he said that it was a secure election. I
15 think even afterwards I think he said it was the -- you know, echoed my statements of it
16 being a secure election.

17 Again, I don't know the -- I can't tell you the specific day or venue or -- we did have
18 that week, though, I don't know if it was the next day, but -- oh, shoot, I'd have to go
19 back. But he mentioned just how secure the election was at the DHS event, like the
20 State of the Homeland event or whatever that was held at St. Elizabeth's. It was about
21 that time.

22 Q Take a look at exhibit 4 in your binder.

23 A Uh-huh.

24 Q It looks like this version of this document came out of a court file. That's
25 that writing on the top. But have you seen this statement before?

1 A I have.

2 Q What is it?

3 A This is a statement that was issued on the 12th of November by the
4 Joint -- or by the Joint Executive Committees of the Sector Coordinating Council and the
5 Government Coordinating Council. So every critical infrastructure sector has a GCC and
6 an SCC. SCC is Sector Coordinating Council. GCC is the Government Coordinating
7 Council.

8 And those groups are comprised for the government, any State or Federal
9 Government partners that may be involved in the critical infrastructure protection
10 mission in that sector. The Sector Coordinating Council is the private sector side or the
11 nonprofit side. The Executive Committees' membership are voted in or selected by the
12 participating organizations in the councils.

13 And they came together in the wake of the 2020 election and they developed the
14 statement that says, as you see in this last line, "There is" -- or not this last line, but the
15 bolded line: "There is no evidence that any voting system deleted or lost votes, changed
16 votes, or was in any way compromised."

17 That was the assessment of the practitioners. The frontline practitioners
18 included election directors at the State level, secretaries of state, voting system
19 executives, government -- Federal Government employees.

20 I did not draft this. It came to me after it was drafted. I looked at it. I said,
21 this is a consensus statement built by the practitioners. I don't have anything to counter
22 or disagree with this, so -- and they asked me for approval to release it. And I said, yeah,
23 sure, I approve.

24 Q Do you know who did draft it?

25 A It was built by committee. The CISA representative to the Executive

1 Committee was Bob Kolasky, the career employee that's the Assistant Director of the
2 National Risk Management Center.

3 Do I know who put each word in there? No.

4 Q And was Mr. Kolasky, not just for the purposes of this statement, but
5 generally the CISA representative on the Coordinating Council?

6 A He was the senior representative, but the Coordinating Councils are
7 supported and facilitated by CISA employees as a part of the Critical Infrastructure
8 Protection Advisory Council structure, which is a statute that allows for, you know,
9 collaboration in an antitrust-free space. And CISA has the statutory authority to
10 facilitate and monitor. But, like I said, Kolasky was the senior here.

11 Q So you were not part of the council?

12 A I was not part of the council, no. I'm not part of any councils. I chair the
13 Federal Senior Leadership Council, which is a -- all the Federal Government partners that
14 sit on top of these structures.

15 Q Do you know why the statement of this -- of the Coordinating Council was
16 issued on CISA letterhead?

17 A Because it was a statement from the Coordinating Committees, and CISA is
18 the convening authority for the committees and -- or the councils and the committee.
19 So it would not have been out of the ordinary to host a statement as a member of the
20 committee. And I suspect that National Association of Secretaries of State, as a member
21 of the committee, NASED, as a member of the committee, would have similarly hosted
22 and promoted.

23 Q I know you said you didn't draft this document. Are you aware of the
24 impetus for this document? Do you know what caused the Council to convene to issue
25 such a document?

1 A The specific impetus I know. I think I may have asked Masterson, Matt
2 Masterson and Kolasky, you know, are the committees going to put anything out?
3 Might they put anything out? And then there was a resulting document.

4 Q Were you personally of the view that a statement regarding the security of
5 the election should be put out?

6 A I was of the view that a statement from the practitioners that had the
7 visibility into how the election was conducted, that gave their perspectives, you know,
8 whether it was CISA, from viewing the intelligence and operational activity from the
9 election equipment, yes, that that would be helpful.

10 Q Why did you think it would be helpful? What was going on at the time that
11 caused you to think that a statement like that would be helpful?

12 A There are significant -- there were a bunch of claims that votes -- that
13 machines had been compromised and votes were being flipped and things of that nature.

14 Q And I know the various constituents here have their own perspective and
15 what's important to them as to why they might have participated. But from CISA's
16 standpoint, did you consider it part of CISA's mission to try to address the concerns that
17 were -- address at some level the concerns that were being raised that you just
18 described?

19 A Again, I think where there's disinformation associated with the secure
20 conduct of an election, where there are claims that, without any sort of support or
21 evidence, that were catching -- not just catching but that were fairly pervasive, again, I
22 thought it would be part -- it's part of the critical infrastructure protection mission to
23 provide factual authoritative information about how things actually worked.

24 Q At the time that you reviewed this statement, did you believe that that
25 bolded sentence -- and I didn't do that bolding. I'm not sure -- let me ask you this: Do

1 you know if that was a bolded --

2 A I think we did that. Well, "we," I think the committee did that.

3 Q So the statement that was issued you believe had that sentence in bold?

4 A Yes.

5 Q Okay.

6 A That's my recollection.

7 Q When you read that statement, did you believe that that was true, from your
8 perspective?

9 A Yes, yes.

10 Q Did you believe it was controversial?

11 A I --

12 Q That's maybe a bad question. I'm going to withdraw that because -- yeah,
13 I'm going to withdraw that.

14 Mr. Walden. Thank you.

15 BY MR. KREBS:

16 Q It's certainly contrary to what you had been seeing or hearing in media or on
17 the internet?

18 A It was certainly contrary to things like HAMMER SCORECARD.

19 ██████████ Let's go off the record for one second.

20 [Discussion held off the record.]

21 BY ██████████

22 Q I'm sorry, do you remember the question, because I don't?

23 Mr. Walden. Yes. You had just withdrawn a question about whether or not he
24 thought the bolded statement was controversial.

25 ██████████ Yes, and then I -- I did do that.

1 BY [REDACTED]

2 Q And then I said that certainly there were statements being -- that were out
3 in the media or on the internet that were contrary to this. And I think you were just
4 starting to say something.

5 A Yes, specifically HAMMER SCORECARD was one of the claims out there, that
6 there was a supercomputer and software program that was changing votes.

7 Q As you sit here today, do you have any -- you know, with a year -- more than
8 a year sort of hindsight, do you have any doubts about the accuracy of that bolded
9 statement?

10 A Absolutely not. In fact, I'm more convinced that it's true, if that's possible.

11 Q Has anyone ever presented you with evidence that you think would
12 undermine that conclusion?

13 A No, none.

14 Q Were you ever told by anyone within DHS leadership that that bolded
15 statement was inaccurate?

16 A The only thing that I recall is a statement that, well, what if evidence comes
17 along later that may disprove that statement? So why would you issue that statement if
18 something down the road could be contrary?

19 Q Who made that statement to you?

20 A That was Chad Wolf.

21 Q When?

22 A Right around the time of the 12th or the 13th, I think.

23 Q What was your response?

24 A If additional evidence or information becomes available, we'll investigate,
25 and we can amend and -- as necessary. But based on available information now, what

1 we know, what we see, this is accurate. And it has held up.

2 Q Did you discuss with Mr. Wolf your view that it was important in terms of
3 CISA's mission, as you just described a few minutes ago, to try to address misinformation
4 that was out in the public sphere?

5 A Specifically, I don't recall. I think that was generally part of the game plan
6 and approach to the 2020 election. It was not just the technical piece, but the
7 perception hack, the disinformation in providing accurate information about what we
8 know happened with the election to the American people.

9 Q I guess what I'm getting at, and I don't want to put words in your mouth, but
10 when he raised concerns about other information maybe coming out that would render
11 this inaccurate, did you push back along the lines of, yeah, but this is important, I mean,
12 this is helpful to address what's going on out there and to try and deal with
13 misinformation; you know, words to that effect?

14 A No, I -- so, to just kind of be a little bit more, you know, perhaps charitable to
15 Chad, I mean, he was asking, you know this to be true -- as I understood it, you know this
16 to be true. What if something -- you know, what if it ends up not being true?

17 He wasn't challenging us necessarily. He was just trying to work through the
18 decision process. And my point was, you know, here's our game plan. If there's
19 additional information, we will investigate and we will work with, you know, our partners,
20 certainly in the FBI, and issue -- you know, continue to keep the American people
21 updated. But in the meantime, it is important to put out the perspective of people that
22 actually conduct elections on what happened, in the face of these -- the growing claims
23 that, absent evidence, something did happen.

24 Q What was Mr. Wolf's response to that?

25 A Okay.

1 Q Did you sense that he was on board and understood and accepted your
2 explanation or justification for the statement?

3 A He didn't give any indication otherwise at the time, that I recall at least.
4 But, again, I was exceedingly confident in the authority of the agency and my authority as
5 the director that I wasn't looking for authorization or approvals. We were executing the
6 game plan.

7 Q Did Mr. Cuccinelli raise concerns with you about this statement after it was
8 issued?

9 A I don't recall. I don't know if I saw Ken after election day again.

10 Q That was going to be my next question. Do you recall any conversation
11 with Mr. Cuccinelli after election day but before you left the agency?

12 A Not that I recall. I mean, I think -- hold on.

13 So, no. The answer is still no.

14 Q I think you mentioned --

15 A Can we go -- can I talk to them real quick? This is off -- can we go off the
16 record?

17 [REDACTED] We are off the record.

18 [Discussion held off the record.]

19 [REDACTED] We're back on the record.

20 BY [REDACTED]

21 Q Again, I forgot what question was pending.

22 A So it's a combination of kind of try stay in your lane stuff and, you know,
23 what Ken -- again, I did not talk to Ken, as I recall at least. There may have been a phone
24 conversation or seen him in passing, but I don't specifically recall a meaningful
25 conversation about any of this stuff between election night and my termination.

1 You know, the one observation I have is that Ken was -- you know, election night
2 he was guest appearing on conservative radio shows from the CISA building, you know, at
3 least three or four different ones. And then about this time or -- again, I'm not
4 attributing this to Ken exactly, but there were leaks coming out from the Department to
5 media -- CNN, Newsmax, CBS -- about CISA. And I don't recall if it was directly me, but,
6 you know, what CISA's mission was. And that continued after I was fired.

7 Q Negative --

8 A Yes.

9 Q -- stories?

10 A To your point of stay in your lane, that's -- you know, fraud -- domestic fraud
11 is not CISA's mission, which the clear response there is that nor did we ever claim it to be.

12 Q And in the statement that we're looking at, do you understand that to be
13 making statements or reference to --

14 A Nope.

15 Q -- election fraud?

16 A Nope.

17 Q Okay. It does say: "no evidence that any voting system deleted or lost
18 votes, changed votes, or was in any way compromised." What do you understand
19 "voting system" to refer to there? I know you didn't draft this document, but what's
20 your understanding?

21 A The technology. But -- I did not, but the actual people that conduct
22 elections. And so, in their parlance, voting systems are the technologies, equipment,
23 machines, computers, devices that are associated with the workflow of conducting an
24 election from, you know, the casting, the counting, and the certification of the process.
25 And that's exactly what that means.

1 Q I'm going to jump -- I'm trying to stay roughly chronological, but jumping a
2 little bit out of order in terms of subject matter, because we're going to come back and
3 talk about the fallout from the statement in a moment. But take a look at exhibit 6,
4 because I think chronologically it's probably our next -- next in order.

5 So this looks like, starting at the bottom -- and I think this is complete. I don't
6 think I cut off any part of the relevant discussion. So the first email in the chain is
7 November 13th at 10:14 a.m. Do you see that?

8 A Uh-huh.

9 Q It's from AS1. Who do you understand that to be?

10 A Acting Secretary. S1 is Secretary. A is Acting. Chad Wolf.

11 Q Okay. So this is from Chad Wolf to you on Friday, November 13th?

12 A Uh-huh.

13 Q Do you recall this email?

14 A I do.

15 Q And is the document that's behind -- the immediate -- the document that I
16 have immediately behind this --

17 A Right.

18 Q -- which we're calling 6A, it's a two-sided page that's sort of fuzzy. The
19 image is somewhat fuzzy, but a November 13th letter from two Michigan State Senators
20 to Jocelyn Benson, the Secretary of State. Do you recall, was that the attachment to the
21 November 13th email?

22 A That is my recollection, yes.

23 Q Do you know Jocelyn Benson?

24 A I do.

25 Q Is she a person that you worked with in connection with your election

1 security efforts at CISA?

2 A She was one of the senior election officials throughout the country, one of
3 the many secretaries of state. And, yes, she was one of the secretaries of state that we
4 worked with. I didn't work with her particularly closely before the election, but the
5 team worked with her team. My team worked with her team.

6 Q Okay. And I can see that you responded to Mr. Wolf within 3 minutes or so
7 of getting his email. And you say that: "We are aware of many of those claims and
8 have discussed with Michigan over the last week, with Michigan addressing most of
9 them."

10 A Uh-huh.

11 Q Tell me about your discussions with Michigan authorities leading up to the
12 receipt of this -- or, you know, prior to the receipt of this email and letter.

13 A So, basically, what would happen is, as any -- as I already mentioned, as any
14 sort of issues would pop up or be, you know, noticed, detected in the news,
15 we -- someone at the Matt Masterson level or down would reach out to the State, their
16 designated point of contact or his relationship, and say, hey, seeing this is getting
17 reported, what's going on, and do you have anything that you've issued, any statements,
18 are you going to issue a statement? And so that would then feed back to us, and, you
19 know, okay, great.

20 And generally, where we're trying to end every one of those engagements was, is
21 there something that we need to be worried about here? And in the case of Antrim
22 County and the -- specifically point one and the database issue, no, they caught it. It
23 was a database configuration issue. They didn't update for that precinct. It was
24 detected. They reconfigured and the votes are accurately counted.

25 Q And you had had that Antrim County discussion before you ever got the

1 email from Mr. Wolf?

2 A Yeah. I mean, that was November 7th. It actually happened earlier than
3 that, but -- I don't recall specifically what the certification deadline is for Michigan, but
4 they caught it fairly early on.

5 And, again, it was -- it was just sloppiness at the programming level with the
6 database. They saw, oh, basically the way that -- they were counted accurately, but
7 when they were deposited into the database for tracking purposes, they had
8 not -- basically, the columns were not appropriately set. Went back through, said, oh,
9 didn't update this database. Updated it. Boom, the votes come, as unofficial but
10 accurate.

11 Q And -- sorry.

12 A And that sort of process happens through canvassing. You catch if there
13 are mistakes, but there was no malicious intent here.

14 Q And it looks as if, based on the next email in the chain, and you say it got
15 stuck in your outbox, so maybe you can help me on sort of when you think you drafted it,
16 you know, relative between Friday and Monday.

17 A It was either -- either Friday afternoon or over the weekend.

18 Q So I guess what I'm getting at is, I'm not going to -- you know, the exact time
19 or day even doesn't really matter, but I'm curious as to whether -- how promptly
20 generally you were able to track down the information that you needed to address the
21 concerns in that letter.

22 A I got what I needed from Masterson probably within a matter of an hour.
23 Again, we were aware of these things. Some of them fell outside of, you know,
24 the -- the -- you know, I'll -- you know, when you talk about official intimidation and
25 interference with lawful election challengers and poll watchers, I would -- I would say

1 that -- you know, if we're talking about lanes, I would say that that's not something that
2 we would typically track, because it's -- it's not directly related to the infrastructure. But
3 it was in the -- it was in the -- it was in the letter. So based on what we understood,
4 based on what Michigan has posted, what they gave to us, we provided it back.

5 And I think really what happened here more than anything probably is that the
6 White House sent this to Chad, said, Chad, what's going on? I want all of these things
7 addressed. We gave them the information back.

8 Q And you think that the body of that Monday, November 16 email probably
9 came to you from Matt Masterson, in terms of tracking down the PDFs?

10 A Yeah, I mean, if I -- do I think that -- you know, I think what happened is I got
11 the one, two, three, four links, that content from Matt or the team, the Election Security
12 Initiative team, and then I dropped a preface on and the front matter and sent it up.

13 Q Okay. And I can see -- as we were talking about the other issues, you were
14 flipping through, and you can see what we're calling 6B is the posting regarding Antrim
15 County.

16 A Right.

17 Q And 6C is a more general posting regarding the absentee ballot process.

18 A Right.

19 Q That my understanding is, although it's not dated, that this --

20 A The TCF Center thing, yeah.

21 Q This information was on the State of Michigan's website on November 16th.
22 It existed at the time.

23 A Right.

24 Q The link I think in your letter is dead at this point, but --

25 A Okay.

1 Q -- that's my understanding.

2 A Okay.

3 Q So do you think you saw these two documents, 6B and 6C, before you
4 responded to Mr. Wolf?

5 A Yes.

6 Q And from your perspective, did it resolve the -- other than the observing of
7 intimidation of poll watchers and things that I think you said might be outside the lane of
8 CISA or are outside the lane, did you feel that this material you got from the Secretary of
9 State's office or their website addressed the other -- the sort of cybersecurity claims that
10 were being made?

11 A I was confident that the matter was closed. But whether that addressed
12 the conspiracy theorists out there, that's a different matter.

13 Q Did Mr. Wolf respond at all to your --

14 A Not that I recall.

15 Q -- Monday email?

16 A Not that I recall. Certainly not with any followup.

17 Q My understanding is the next day you were terminated.

18 A Sounds right.

19 Q Okay. Take a look at back at exhibit 5. It's a letter dated November 17th
20 from John McEntee to you. Have you seen this before?

21 A You know, in the exhibits that were provide --
22 Mr. Walden. I just want to say, could you clarify, before today or at the time?

23 BY [REDACTED]

24 Q Before today, have you seen this document?

25 A So I saw -- you know, I saw this yesterday or Tuesday. And I'll admit that

1 when I saw it then, it was like, I don't know if I've seen this before. So I know that in the
2 exhibits provided that it was in an attachment to an email that was sent to me from
3 someone, but you have to keep in mind, even whenever that was dated, that email
4 was -- the date stamp on that, I probably got a thousand emails that night.

5 And I actually put down my work device and wasn't using my -- I mean, I
6 considered myself terminated. So I don't know if I actually even looked through all my
7 email that evening.

8 Q Got it. So it's possible that this termination letter was transmitted to you
9 on December -- on November 17th, 2020, but you don't recall or you did not see it then?

10 A Not that I recall.

11 Q Okay. How did you learn that you had been terminated?

12 A Someone sent me a text that said, You just got fired on Twitter. And my
13 immediate reaction was like, nah, nah, you're thinking about -- you read that article last
14 week from Natasha Bertrand in Politico. And lo and behold, I pull up Twitter and there it
15 is, 7:05, 7:06 p.m.

16 Q What did you pull up on Twitter?

17 A The President's tweet. It was two tweets, and it says basically because I,
18 you know, made statements that were untrue that I'd been terminated as Director of
19 CISA.

20 Q And did you sort of take that as sort of actionable or did you seek out some
21 confirmation from one of your superiors in the Agency or the Department?

22 A I immediately called Chad Wolf. He was not available. So I put a call in, I
23 guess -- as I've been refreshed from the exhibits, I guess I called the watch -- the DHS
24 NOC, the Ops Center, and said, hey, trying to get ahold of the Secretary. Called him.
25 He called me back.

1 Fairly soon after, also -- you know, you'd have to look at -- I don't recall the actual
2 sequencing, but then I called my chief of staff. I called -- talked to Matt Travis, and I
3 think I also probably talked to Brandon Wales.

4 Q So you determined that the tweet was actionable, that you had, in fact, been
5 terminated? There have been examples of Presidential tweets that I've read or heard
6 about that were actually --

7 A There was zero ambiguity, zero ambiguity from the tweets.

8 Q And you were a Presidential appointee, so presumably the President has the
9 authority to fire you whenever he wants.

10 A And from past practice, you know, under -- even -- yes. So I had enough to
11 understand that I was fired.

12 Q Okay.

13 Mr. Walden. Just so the record is clear, did you have a conversation with Chad
14 Wolf where he confirmed it?

15 Mr. Krebs. Yes. And he said, oh -- something to the effect of, oh, god, that
16 wasn't supposed to happen like that.

17 BY [REDACTED]

18 Q Okay. Did he give you any explanation as to why it happened? Not why
19 the tweet happened, but why you were being terminated.

20 A I don't recall specifically what any sort of -- but I think it was fairly obvious,
21 and obvious being that, you know, we were providing factual information about the
22 security of the election.

23 Q In your mind -- because you're saying it was obvious to you, in your mind,
24 was it tied to this November 12th statement that we were looking at or something else or
25 an aggregation or accumulation of such statements?

1 A I would not attribute it to any single event.

2 Q Okay. Did anyone ever tell you, you know, that November 12th statement,
3 that -- you shouldn't have sent that out, that's the reason you got fired?

4 A Not that I recall.

5 Q And it's not your understanding that it was that -- standing alone, it was not
6 that statement?

7 A I don't have any information. I was never provided any information that
8 that was a --

9 Q Okay. I said I was going to try and proceed chronologically, but I realize I
10 have an exhibit in here that is a bit out of order, and it's just sort of a random question for
11 you. It's exhibit 7.

12 A Uh-huh.

13 Q This appears to be an email from AS. And my understanding is that the
14 redaction inadvertently deleted the number 2. So it should be from AS2.

15 A Uh-huh.

16 Q Do you know who AS2 is?

17 A AS2 would be Ken Cuccinelli.

18 Q And you can see it's signed "See you shortly. Ken."

19 A Right.

20 Q Do you have any recollection of getting this email from Mr. Cuccinelli on
21 November 3rd?

22 A I do not.

23 Q Do you have any understanding of what this email refers to?

24 A One query I picked up from the congressional call was regarding the
25 CISA.gov/rumorcontrol page.

1 So throughout the -- the congressional call, I will stipulate that I don't know
2 specifically there, but throughout the day, in addition to the press calls, we were doing
3 updates to congressional members and staff.

4 And we had actually been -- I had been providing briefings to Congress for months
5 about our preparation. And those sort of died off as an interagency prior to, you know,
6 I'd say right around August, but we continued as an agency to give those on a biweekly
7 basis probably. And, you know, we'd open it up to -- we do a House call and then we do
8 a Senate call. And, you know, again, still in the middle of COVID. We'd be kind of
9 doing these all over the place.

10 So on the day of the election, it may have even been -- I think there was at least
11 one the day of the election, and we were just kind of talking about, here's what we're
12 seeing out there. And we knew the issues that were popping up on that day, and they
13 were, you know, like poll book issues or power outages or things like that. And we'd
14 say, hey, look, these are the key things we're seeing. But other than the
15 adversary -- you know, other than that, we're not seeing any adversary activity. It
16 seems to be actually a pretty quiet and calm election.

17 And I don't recall specifically what the question is or who asked it, but I assume
18 something came up like, hey, I'm hearing about this rumor control thing, tell me about
19 that. And --

20 Q Okay.

21 A That's my understanding -- my recollection, rather.

22 Q You don't have a recollection of a specific aspect of a rumor control page
23 that was being inquired of, just --

24 A Not that I recall.

25 Q Okay.

1 A No.

1

2 [1:16 p.m.]

3

BY [REDACTED]

4

Q Okay.

5

6 Okay. I want to go through a couple of points here with you just to get a sense
7 of your familiarity and understanding and what your, sort of, state of knowledge is on
8 this.

8

9 There have been questions raised about Dominion voting machines. You
10 referenced dead foreign dictators --

10

A Right.

11

12 Q -- and so forth. Are you generally familiar with the testing or evaluation
13 that is done on Dominion voting machines by the various States that have used them?

13

14 A Yeah, so my -- it's been a year or so since I've actually jumped into the details
15 of what States do and what the standards are. But, yes, generally speaking, there is a
16 set of voluntary standards that the Election Assistance Commission publishes, there are
17 labs that the EAC accredits, and then there are, in some States, State-specific
18 accreditation labs.

18

19 And so, you know, virtually every State has some kind of testing standard.
20 They're not all the same. Some are more rigorous than the Federal guidelines, and
21 some States, you know, just kind of follow whatever the Federal Government
22 recommends, the EAC recommends. But it's all -- it's kind of a mixed bag across the
23 landscape.

23

24 Q And are you apprised of and typically -- a bad question. Is CISA apprised of
25 whether a particular voting machine has met or not met various State standards, or it's
just sort of up to the States to do what they do?

1 A The States generally do what they do.

2 Q Have you ever been apprised of particular issues that have come up with
3 respect to State testing or State evaluation of Dominion Voting Systems?

4 A Specifically Dominion, I can't recall any specific issue necessarily.

5 I know there was something in Texas about, Texas had a rigorous -- it's not
6 rigorous, but Texas had a set of State requirements that some machines -- I don't recall if
7 it was Dominion or ES&S, but that a system may not have passed the State certification
8 process. But it wasn't necessarily because of any sort of security standard. But I
9 believe, in this case, they did issue -- Texas issued some sort of assessment and
10 decertification of a system. Again, I don't recall if it was Dominion or ES&S.

11 Q Okay. And are you able to say with any degree of certainty that,
12 if -- because it may vary State by State, but that, if a Dominion voting hardware -- because
13 I know there's -- is there software and hardware that's created by Dominion?

14 A Yes. There's machines, and then there's the software that actually sits on
15 top of, in many cases, like, a Windows operating system that's specific to --

16 Q Are you able to say with any level of confidence that -- the fact
17 that Dominion Voting Systems could not have been used in the United States had they
18 not gone through some -- the respective testing protocols of the States in which they're
19 used?

20 A I -- so I --

21 Q Terrible question.

22 A Yeah. So States have certification processes. And, to use the equipment
23 in a State, you have to follow their regime, as I understand it.

24 Q Okay.

25 A Generally speaking. Could there be individual State-by-State exceptions?

1 You know, I don't --

2 Q Yeah. Yeah. Okay.

3 Have you ever had any interactions with a person named Russell Ramsland?

4 A I never have, no.

5 Q Do you know whether Mr. Ramsland ever presented to folks within CISA
6 concerns that he had about electronic voting?

7 A So whether Mr. Ramsland specifically -- and Mr. Ramsland is with ASOG,
8 Allied Security Operations Group. I don't know specifically if Mr. Ramsland briefed any
9 CISA employees, but I believe representatives from ASOG briefed CISA and other DHS
10 employees in the State of Texas.

11 And then, subsequently, as I understand it, he briefed, as encouraged by the
12 Senate Homeland Security Committee, majority staff at the time, under Chairman Ron
13 Johnson -- the Senate staff directed CISA -- requested CISA headquarters personnel, I
14 guess, meet with ASOG personnel to review whatever findings they had.

15 Q Were you part of those meetings?

16 A Absolutely not. I never heard about it until well after I was relieved of
17 duty.

18 Q Would that have been Matt Masterson most likely?

19 A I don't believe so.

20 Q Who do you --

21 A I believe they may have brought in probably some -- there was probably
22 some lower-level career staff and then also some outside consultants that are experts in
23 election technology.

24 Q Okay.

25 So, before we wrap up, I want to ask you about some, sort of, reflections on the

1 2020 election and maybe your thoughts on certain recommendations. I know, in your
2 Senate testimony that we looked at earlier, exhibit 1, you had some bullet-point
3 recommendations that you thought should be considered by the Senate.

4 A Uh-huh.

5 Q And I want to give you a chance to talk about some of that.

6 A Okay.

7 Q There are -- several recent polls have shown that a large percentage of
8 Americans believe that the 2020 Presidential election was stolen. Are you generally
9 familiar with that sentiment?

10 A Yes, I am.

11 Q Do you have a view as to what accounts for that?

12 A My personal, Chris Krebs, belief that the reason particularly that that
13 number is much higher skewed in Republican circles is because Republican officials,
14 senior officials, including the former President, lied to the American people about the
15 security of the 2020 election, that it was stolen. So it's a self-reinforcing cycle.

16 Q Does it concern you, as someone who spent a good part of your professional
17 career dealing with risk generally and election security risk, does it concern you that
18 there's a substantial portion of the American population that thinks that the Presidential
19 election in 2020 was stolen?

20 A Yes.

21 Q Why?

22 A If you don't have confidence in the processes by which we choose our
23 elected officials, those that represent us, then you start to doubt other mechanisms of
24 democracy.

25 And democracy is a -- unfortunately, a contact sport, but also requires active

1 engagement and participation. And so what I fear is that we will see disengagement
2 from democracy that will lead us into, you know, antidemocratic forms of government.

3 Q In your view, what could have been done or can be done to combat the type
4 of disinformation that you're talking about?

5 A So --

6 Q Or keep it from taking hold as it has?

7 A So I'd separate the actual disinfo, in and of itself, but we need to improve
8 upon the structures by which we conduct elections. And I'm specifically talking about
9 the electoral count, or the Electoral Count Act.

10 And Ben Ginsberg had a pretty good op-ed, I think, in the National Review Online
11 last week where he ticks through about a dozen or so things that need to be clarified
12 from that law from the 1860s or whatever it was, you know, including clarifying the role
13 of the Vice President and whether the Vice President is, in fact, just a ceremonial role or
14 not.

15 And, in part, the point that he makes is that, you know, Republicans, in this case,
16 should be careful what they wish for, because in 2024 Kamala Harris is going to be the VP.
17 And so, if they -- you know, they've given a game plan. And, while Pence didn't follow it
18 in 2020, if Kamala Harris followed it in 2024, that obviously wouldn't work to the
19 Republicans. So it's in everybody's interest to actually clarify how the electoral college
20 mechanism works.

21 So, again, start with clarifying the Vice President's role; clarifying how
22 disagreements are adjudicated between the House and the Senate if they have a
23 disagreement; clarify at the State level who the executive is that's responsible for
24 certifying the slate -- because you could see a Republican and Democrat from
25 different -- you know, one serving Governor, the other serving as a secretary of state, and

1 they could each claim to be the executive, and you could have those dueling slates. So
2 clarify who the State executive is; you know, perhaps look at things like increasing the
3 number of Congresspeople that can object to a slate from a State, instead of just one,
4 actually raise the threshold there.

5 So, again, Ginsberg's got a pretty solid list. I encourage every -- you know, that
6 that's in everyone's interest. That's point one.

7 So I think there are a few other things. I think, you know, when you look at all of
8 our ilk, as lawyers, there were a number of attorneys that were involved in filing, as we've
9 seen in Michigan and elsewhere, at least sanctionable lawsuits, but 60-plus that were
10 thrown out. I think we need, you know, to reinforce some of the societal norms in
11 particularly those bodies like bar associations and even, if you look at COVID, with
12 medical licensing boards. There are actually some self-policing and self-reinforcing
13 mechanisms that we're not going to tolerate this and we can police ourselves. So that's
14 number two.

15 Number three, I think -- and these are some recommendations from the Aspen
16 Commission -- you know, some regulation around social media platforms, not in a
17 managing or moderating content perspective, but just from a transparency in how these
18 platforms, you know, enforce their own terms of service and inconsistency. Because
19 there's not necessarily a whole bunch of consistency in how they do things from country
20 to country.

21 And then, you know, lastly, when you just think about -- and this is the hardest
22 part. The hardest part, as I see it is -- this goes back to that point about democracy.
23 You know, democracy and elections require both parties commit to the democratic
24 process and that they commit to honoring the outcome of a legitimate election. If one
25 decides not to participate in that, then that's not much of a democracy. So actually

1 reinforcing committing to elections.

2 Now, how do you enforce that? Obviously we see, right now, we're not getting a
3 whole lot of enforcement. There's no mechanism to hold those that are making these
4 claims, other than at the ballot box. But even that's not good enough, because those
5 structures here are not exactly holding some of these elected officials accountable for
6 continuing to propagate claims.

7 So this is hard. You know, a lot of, kind of, the Speech and Debate Clause gives a
8 lot of coverage for, you know, Members of the Congress to make these claims. So I
9 think we have to continue investigating and, you know, developing options to help to
10 hold these folks, particularly elected officials, accountable.

11 And the last thing I'll say is that, you know, this is a -- not only, you know, it's a
12 contact sport, but it's also requiring whole of society to recommit. So, you know,
13 something to the order of, you know, business leaders tend to be more higher respected,
14 regarded, whatever, and so businesses need to take a hard look at, you know, from a
15 political -- you know, post-Citizens United, you know, if they're contributing to political
16 campaigns, that, you know, they should not be contributing to campaigns of candidates
17 for office that continue to promote baseless conspiracy theories about the theft of
18 election. I think they're contributing to the downfall of America.

19 Q Do you think the government or we, as a society, or maybe the government,
20 in terms of CISA, has done enough to counter the false information that's come out with
21 respect to the 2020 election?

22 A I think that, under the constructs of the First Amendment, there is only so
23 much the government can do besides provide accurate information on how elections are
24 conducted and, you know, what has happened in the past and what will happen going
25 forward.

1 But you don't overcome disinformation with more information, with truth. You
2 have to get it at a much, much, much more foundational level and undercut some of the
3 structural incentives for those that continue to promote it and those that want to.

4 Q But -- and I appreciate your thoughtful comments on this, and I don't want
5 to sort of belabor it, but, you know, we started the discussion today, or this interview,
6 talking about, sort of, some of the threats from Russia to sow distrust and so forth. Did
7 you ever in your wildest, sort of, imagination think in 2017, when you were thinking
8 about how to deal with disinformation and how it might -- I think you called it a cancer
9 that could sort of grow and erode American values -- that we'd get to a point where
10 two-thirds of one of the major political parties in the country don't believe in elections
11 anymore or don't believe they can be trusted?

12 I mean, it seems as that -- I mean, if the Russians were doing this and got to that
13 level of penetration, would that be alarming --

14 A Of course it's alarming. But even if it is Russian disinformation that an
15 American citizen picks up and then promotes on Twitter, it's still an American citizen
16 expressing their First Amendment views. And that's --

17 Q I guess what I'm asking --

18 A -- permissible.

19 Q -- is: Have your worst fears, when you set out on this mission of trying to
20 sort of protect the integrity of elections, in some sense been --

21 A It's worse than I thought.

22 Q Okay. Because the level of penetration, or just the --

23 A Active participation by the political class in American democracy.

24 Q And do you think that creates greater challenges than even dealing with, sort
25 of, a malign foreign actor?

1 A Much, much, much, much, much harder because of the First Amendment
2 issues, because there's no accountability measures, there's nothing we can, again, do
3 right now to -- you know, there are things that, if it was a Russian doing what the former
4 President continues to do to this day, then there are mechanisms in place to intercept
5 and intervene in that information. But the fact that it's an American citizen promoting
6 their own view, which is their right under the First Amendment, even if it's cancerous and
7 contrary to democracy, there's not a whole lot to do, other than -- sorry.

8 Mr. Walden. No, no, you're okay. You misread me.

9 Mr. Krebs. But this is -- you know, as soon as you get, you know, an interested
10 party as the target of the defamation, like Dominion Voting Systems, they have legal
11 recourse. They can sue for \$1.3 billion, as they are. But the problem here is that it's
12 going to take multiple years to settle that, or not settle, but actually come to, you know,
13 some finality if it makes it that far. And, by then, the damage is done.

14 ████████ Well, on that somewhat depressing note, I think we'll --

15 Mr. Krebs. Welcome to my life.

16 ████████ I'm sorry?

17 Mr. Krebs. Welcome to my life. Yeah.

18 ████████ -- we'll call it a day.

19 So let's go off the record.

20 [Whereupon, at 1:34 p.m., the interview was concluded.]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Certificate of Deponent/Interviewee

I have read the foregoing ____ pages, which contain the correct transcript of the answers made by me to the questions therein recorded.

Witness Name

Date